DOI 10.15622/ia.23.5.6

R. JENIFER, V.J. PRAKASH

RIVEST-SHAMIR-ADLEMAN ALGORITHM OPTIMIZED TO PROTECT IOT DEVICES FROM SPECIFIC ATTACKS

Jenifer R., Prakash V.J. **Rivest-Shamir-Adleman Algorithm Optimized to Protect IoT Devices from Specific Attacks.**

Abstract. IoT devices are crucial in this modern world in many ways, as they provide support for environmental sensing, automation, and responsible resource conservation. The immense presence of IoT devices in everyday life is inevitable in the smart world. The predominant usage of IoT devices lurks the prying eyes of intentional hackers. Though there are several precautionary security systems and protocols available for generic wireless networks, it is observed that there is a need to formulate a state-of-the-art security mechanism exclusively for IoT network environments. This work is submitted here for the betterment of IoT network security. Three dedicated contributions are integrated in this work to achieve higher security scores in IoT network environments. Fast Fuzzy Anomaly Detector, Legacy Naïve Bayes Attack Classifiers, and Variable Security Schemer of Rivest-Shamir-Adleman algorithm are the novel modules introduced in this work abbreviated as ASORI (Attack Specific Security Optimized RSA for IoT). Captivating the advantages of the onboard IoT certification mechanism and selecting a dynamic security strategy are the novelties introduced in this work. ASORI model is tested with industrial standard network simulator OPNET to ensure the improved security along with vital network performance parameter betterments.

Keywords: Internet-of-Things (IoT), network security, fuzzy anomaly detection, Naïve Bayes classification, RSA.

1. Introduction. An IoT device is an electronic device that is embedded with one or more sensors, internet connection ability, data processing ability and optional drivers or actuators [1]. Literally, they are all small embedded devices equipped with at least IEEE 802.11 wireless communication capability. IoT devices are omnipresent these days, and that takes place in almost every automation and other operations [2]. From agricultural to industrial automation, the Internet of Things (IoT) has reformed several industries by combining daily objects and devices with the Internet, enabling them to collect, share, and exchange data. IoT applications span a wide range of sectors, from smart homes that allow remote control of appliances and thermostats to healthcare where wearable devices monitor vital signs and transmit patient data for remote diagnosis. Industrial IoT optimizes manufacturing processes through real-time monitoring of machinery and predictive maintenance, while agriculture employs IoT for precision farming, optimizing irrigation and monitoring crop conditions. Smart cities utilize IoT to enhance urban services, such as intelligent traffic management and waste management systems [3]. As IoT continues to evolve, it holds the potential to enhance efficiency,

convenience, and sustainability across numerous domains, transforming the way we interact with the world.

An attack on IoT is one of the spiteful attempts to utilize weakness in internet-connected devices. Internet-connected devices can be smart home devices or industrial control systems, even medical devices [4]. If an attacker could obtain control of any of these devices, he could abuse sensitive data or even destroy a system. Since IoT devices are cost effective the computational resources are used to be very limited. This limited resource nature is prone to several attacks that cause network instability [5]. The heterogeneous property of IoT nodes is also an important gateway to malicious attacks. Following a standard static security method is not sufficient to maintain acceptable security in IoT network environments [6]. Most modern life-supporting systems are developed using IoT devices. Any possible threat to these IoT devices can cause severe physical consequences. Therefore, it is important to devise a precise lightweight dynamic security system for IoT network environments.

2. Existing Methods. A set of relevant existing methods is taken here to understand the fundamental principles, methodologies, advantages and limitations of IoT network security. Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol [7], An authentication information exchange scheme in WSN for IoT applications [8], Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN [9], A secure IoT-based mutual authentication for healthcare applications in wireless sensor networks using ECC [10], and Towards an improved energy efficient and end-to-end secure protocol for IoT healthcare applications [11] are the methods examined in this work.

2.1. Securing Wireless Sensor Networks against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. In 2019, in study [7] the authors presented Abnormal Sensor Detection Accuracy with RSA (ASDARSA) work to protect IoT networks in particular for Denial of Sleep (DoSL) type attacks. Energy and Distance-based cluster head selection methodology, and RSA Cryptography based interlock protocol are the two phases defined in ASDARSA work. The standard RSA algorithm is used in this ASDARSA work for key generation, encryption and decryption. The novelties identified in ASDARSA work are an introduction to an energy consumption model, a Cluster head selection procedure, a dedicated DoSL prevention procedure, and cluster-level node authentication. NS-2 network simulator is used to evaluate the performance parameters such as throughput, packet delivery ratio, detection range, residual energy and lifetime of the network. Preliminary assumptions such

that nodes are homogeneous and placed statically, cluster head can only communicate with the base station, and a constant communication rate is followed in ASDARSA work.

Higher security against DoSL-type attacks is the noted advantage of ASDARSA work whereas decreased network performance and lack of security against modern attacks are the identified limitation.

2.2. An authentication information exchange scheme in WSN for IoT applications (AIES). AIES work is introduced by the authors in [8] to confront node capture attacks in IoT-based wireless sensor networks. Dedicated procedures for the System setup phase, a new association scheme and a dynamic contracting mechanism are introduced in AIES. The sensor registration phase, User Registration phase, login session, Authentication, and key agreement phase are described clearly in AIES work. Along with node capture attacks, AIES also resists Replay attacks and Sensor impersonation attacks. AIES work also facilitates anonymity to protect user information. The security evaluation is done by BAN logic.

The achievement of security against node capture attacks is the advantage of AIES work. Missing assessment against essential network performance metrics such as Throughput, Communication Delay and Packet delivery ratio are identified as the limitation of AIES work. Security against several modern attacks is not included in AIES work, which is another observed limitation.

2.3. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Paper [9] proposed a fog-assisted secure healthcare data aggregation scheme represented as Enhanced Healthcare Data Aggregation (EHDA). EHDA work uses the Fog server to minimize the storage, communication and energy overheads. EHDA uses peer-to-peer communication between healthcare IoT devices and wearable IoT devices to aggregate data. As per EHDA work, the fog server receives the aggregated data from IoT devices and stores it in the local repository. Thus, the cloud server can extract the required data from the fog server and store it in cloud storage. Individual algorithms are provided in EHDA work for message reception in the Aggregator node, and Aggregator node to Base station. The lightweight cryptography scheme reduces the energy overhead. NS2.35 simulator is used to measure the discussed overheads in EHDA work.

The achievement of reduction in storage, communication and energy overheads are the stated advantages of EHDA work. The lightweight cryptography diminishes security is one of the limitations of EHDA. Network performance metrics such as throughput, Packet delivery ratio, and

communication delay are not evaluated during the experiments carried out for the EHDA work.

2.4. A secure IoT-based mutual authentication for healthcare applications in wireless sensor networks using ECC (SIMA). SIMA work is proposed by the authors in paper [10] to improve security in Wireless Medical Sensor Networks (WMSN). SIMA ensures a new privacy-perceiving user authentication scheme with the help of Elliptic Curve Cryptography. A lightweight authentication scheme is introduced in SIMA work to withstand Smartcard stolen attacks, Insider attacks, User impersonation attacks, Gateway node impersonation attacks, Sensor node impersonation attacks, forward secrecy attacks, and replay attacks. BAN logic and the Random Oracle model are used to demonstrate the security characteristics of the SIMA model. AVISPA simulation tool is used to perform a clear security analysis of SIMA work. Dedicated methods are provided for standard network authentication phases such as the System initialization phase, User registration phase, Sensor node registration phase, gateway registration phase, Login phase, Authentication phase, Password revocation phase, and Dynamic node adjunct phase.

The achievement of less computational and communication overheads is the advantage of SIMA work, whereas, attack detection accuracy and precision are not measured during the evaluation process. Common network performance measurement metrics such as throughput, latency and packet delivery ratio are not discussed in SIMA.

2.5. Towards an improved energy efficient and end-to-end secure protocol for IoT healthcare applications. An Asynchronous duty cycle medium access control protocol is proposed by the author in [11] in the name Local Coordination XMAC (LCX-MAC) to reduce data transmission delay and energy. LCX-MAC method uses a set of timers to operate and to reduce power consumption by periodically operating nodes in Sleep mode, Data availability, back-off timeout, Channel status, Early acknowledgment and Data transmission status. The regular duty cycle of MAC protocol is modified with the Markov model to optimize the Sleep/Wake time cycles. Throughput, communication delay and Average energy consumption are calculated using the formula.

The improvements in Throughput, communication delay and energy are the stated advantages of LCX-MAC work. The entire parameters computations are performed using calculations. There are no simulation-based results produced in the evaluation process – which is the limitation of this work. The Security aspect of LCX-MAC work is totally absent in the evaluation process.

The used methodologies, Advantages and Limitations of the existing works are enumerated in Table 1.

Table 1. Existing works, Methodologies, advantages and limitations

No.	Work	Year	Methodology	Advantages	Limitations
[7]	Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol	2019	Energy-Distance-based Clustering, RSA	Security against DoSL	Vulnerable to Probe, U2R attacks
[8]	An authentication information exchange scheme in WSN for IoT applications	2020	Legacy association scheme, Dynamic contact mechanism	Security against Node capture attack	Impact on network performance
[9]	Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN	2020	Peer-to-peer communication, Fog data aggregation	Reduced communication and Energy overheads	Diminished network performance
[10]	A secure IoT-based mutual authentication for healthcare applications in wireless sensor networks using ECC	2021	ECC-based lightweight authentication	Reduced communication and computational overheads	Low throughput, Attack detection accuracy
[11]	Towards an improved energy efficient and end-to-end secure protocol for IoT healthcare applications	2020	Timer-based node mode control	Better network performance	Compromised security

3. Background. Fuzzy logic and the Rivest-Shamir-Adleman (RSA) algorithm are acknowledged as the background methodologies of the

proposed work. A clear understanding of Fuzzy logic and the RSA algorithm is required to explicate the ASORI work, covered in this section.

3.1. Fuzzy Logic. Fuzzy logic is a mathematical concept and a computing paradigm that deals with reasoning and decision-making in situations that involve uncertainty, ambiguity, and imprecision. It was introduced by Lotfi A. Zadeh in 1965 as an extension of classical (Boolean) logic to handle situations where the boundaries between true and false are not clearly defined. In classical logic, propositions are either true or false, with no middle ground. Fuzzy logic, on the other hand, allows for degrees of truth to be represented. It introduces the concept of membership functions, which assign a degree of membership (between 0 and 1) to an element in a set [12]. These membership functions capture the gradual transition between different states rather than abrupt distinctions. Fuzzy logic is commonly used in control systems and decision-making processes where human expertise and intuition play a significant role. Fuzzy logic stands in between analog and digital signal measurements; and litigations are the best to formulate fast decision-making [13]. The fuzzy logic system is used to select an optimal path for data transmission during uncertainty [14]. The flow of the fuzzy logic process is illustrated in Figure 1.

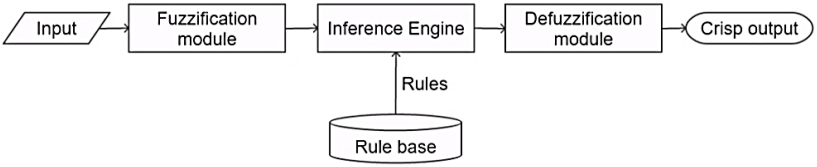

Fig. 1. Fuzzy Logic block diagram

The key idea is to represent the flow of information from input variables through fuzzification, rule processing, inference, aggregation, and finally defuzzification to obtain a crisp output value or action.

3.2. RSA. RSA, which stands for Rivest-Shamir-Adleman, is a widely used public key cryptosystem and encryption algorithm. It was introduced by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977 and remains one of the most important and secure methods for secure communication and data protection RSA is based on the mathematical properties of large prime numbers and their difficulty in being factored [15]. The security of RSA relies on the fact that it is computationally infeasible to factorize a large semiprime (the product of two large prime numbers) into its constituent primes, especially when the primes are chosen to be sufficiently large [16].

RSA key generation:

Step 1: Generate two distinct large prime numbers, as "p" and "q".

Step 2: Compute the product of these primes, "n = p * q", which becomes the modulus used as the public and private keys.

Step 3: Compute the totient of n, denoted as "φ(n) = (p - 1) * (q - 1)".

Step 4: Choose an encryption exponent "e" that is relatively prime to φ(n), typically a small prime like 65537 ($2^{16} + 1$).

Step 5: Compute the decryption exponent "d" such that (d * e) mod φ(n) = 1.

Step 6: The public key is (n, e), and the private key is (n, d)

RSA Encryption:

Step 1: To encrypt a message "M", the sender uses the recipient's public key (n, e)

Step 2: The sender converts the message into a numerical value “m”

Step 3: The sender calculates the ciphertext "C" using the formula: C = (m^e) mod n.

Step 4: The ciphertext "C" is sent to the recipient

RSA Decryption:

Step 1: The recipient uses their private key (n, d) to decrypt the ciphertext "C"

Step 2: The recipient calculates the plaintext message "m" using the formula: m = (c^d) mod n.

Step 3: The recipient converts the numerical value "m" back into the original message format.

RSA is widely used for secure communication, digital signatures, and various other cryptographic applications. It is considered secure as long as the key sizes are chosen appropriately large (e.g., 2048 bits or more) and the algorithms are implemented correctly. However, with the advancement of computing power and algorithms, it is important to keep up with best practices and periodically update key lengths to ensure continued security.

4. Proposed method ASORI. There are three discrete modules formulated to construct the ASORI model. They are Fast Fuzzy Anomaly Detector, Legacy Naïve Bayes Attack Classifier, and Variable RSA Security Schemer. The comprehensive details about the functionalities of these modules are described in this section.

4.1. Fast Fuzzy Anomaly Detector (FFAD). FFAD is designed in a way to identify anomaly network communication attempts. The

incorporation of Fuzzy logic ensures accurate anomaly detection swiftly. FFAD uses Traffic volumes, Baseline traffic, Time of the day, Protocol outliers, Location assessment, change in User privilege, Header interpretation, Payload dissection, Port scanning, Ping sweeps, Connection duration, and Number of connections as the constituents to detect an intruder [17]. These 12 parameters are individually categorized into 4 anomaly severity labels such as Nada, Low, Medium, and High. The severity labels are aggregated for all 12 parameters to detect anomaly network activities. The label weights are assigned from 0 to 3 for Nada to High respectively. Therefore, the maximum label weight ω_{max} is 3.

Traffic Volume(v_T) refers to the amount of data transferred through a node at any particular time. v_t is computed using Equation 1.

$$v_T = I_T \times t, \tag{1}$$

where I_T is the traffic intensity, t is the time.

FFAD measures the traffic volume difference v_{T_d} between the previous network volume v_{T_p}which is measured at a time $t-1$ and the current traffic volume v_T as follows:

$$V_{T_d} = \left|V_T - V_{T_P}\right|. \tag{2}$$

Since the possible lowest traffic volume is 0 in IoT networks, the severity label L_{tr} is calculated by Equation 3.

$$L_{tr} = \begin{cases} Nada\ if\ \dfrac{v_{T_d}}{v_{T_m}} < \dfrac{1}{4} \\ Low\ if\ \dfrac{1}{4} \le \dfrac{v_{T_d}}{v_{T_m}} < \dfrac{1}{2} \\ Medium\ if\ \dfrac{1}{2} \le \dfrac{v_{T_d}}{v_{T_m}} < \dfrac{3}{4} \\ High\ otherwise \end{cases}, \tag{3}$$

where v_{T_m} is the maximum possible traffic volume.

Baseline traffic is the typical network traffic between specific nodes to cluster heads or base stations. FFDA uses the baseline traffic between the cluster heads and base station as in the following algorithm to determine the anomaly severity label.

Algorithm 1. Baseline traffic anomaly severity labeler

Input: Baseline traffic information
Output: Anomaly severity label

Step 1: Let n_{CH} be the number of cluster heads in the network
Step 2: Let Γ be the set of cluster heads with members $\{\gamma_1, \gamma_2 \cdots \gamma_{n_{CH}}\}$
Step 3: Let b_T be the set of baseline traffic set by 1:1 correspondence to Γ with members $\left\{b_{T_1}, b_{T_2}, \ldots b_{T_{n_{CH}}}\right\}$
Step 4: Initialize baseline traffic anomaly severity label L_{bl} = Nada
Step 5: Let L_{temp} be the temporary label
Step 6: $\forall i = 1 \rightarrow n_{CH}$
Step 7: ComputeL_{temp} by Equation 4
Step 8: if $L_{bl} < L_{temp}$, set $L_{bl} = L_{temp}$
Step 7: return L_{bl}

The temporary baseline traffic anomaly severity label is determined by the following equation:

$$L_{temp} = \begin{cases} Nada\ if\ \dfrac{b_{T_i}}{b_{T_m}} < \dfrac{1}{4} \\ Low\ if\ \dfrac{1}{4} \leq \dfrac{b_{T_i}}{b_{T_m}} < \dfrac{1}{2} \\ Medium\ if\ \dfrac{1}{2} \leq \dfrac{b_{T_i}}{b_{T_m}} < \dfrac{3}{4} \\ High\ otherwise \end{cases}. \quad (4)$$

The flowchart for the algorithm 1 is given below (Figure 2).

By this way, the baseline traffic anomaly severity label will get the highest severity index of all cluster head communications with the base station. That is, the baseline traffic anomaly label will get the value of "High" with even a single malicious node entry in any of the clusters in the entire network.

Time of day is one of the important factors in anomaly detection in scheduled communication an IoT network environment. The Time of day anomaly severity Label L_{td} is set to have only two labels in the FFAD module for ease of processing. The assignable labels are Nada and high. For all non-scheduled IoT network nodes, L_{td} is assigned with a Nada label For prescheduled IoT nodes, let Δ_{comm} be the set of preapproved time slots $\{\delta_1, \delta_2 \ldots \delta n\}$. Then for a communication attempt made at a time t_{ca}, the time of day anomaly severity label is assigned as in Equation 5.

$$L_{td} = \begin{cases} Nada\ if\ t_{ca} \in \Delta \\ High\ otherwise \end{cases}. \quad (5)$$

The protocol outlier severity label L_{po} is set to high if a node tries to communicate with another node through a new protocol. Otherwise L_{po} is assigned with the label Nada. Location assessment is used to check whether an intruder node is trying to get into the network.

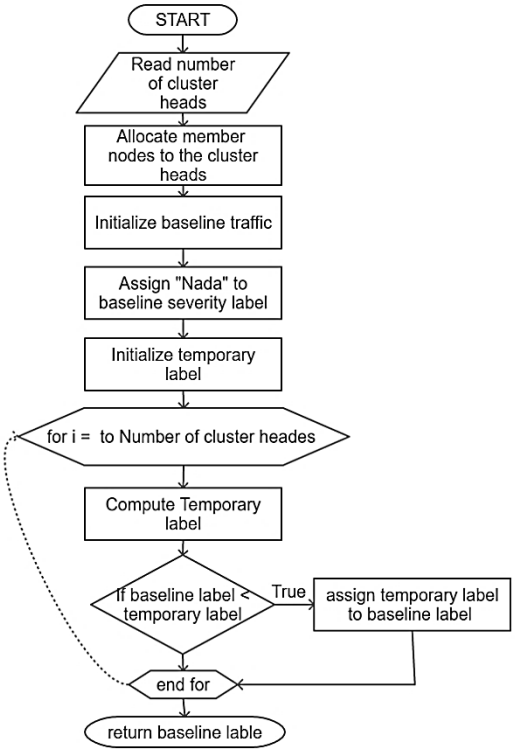

Fig. 2. Algorithm 1 flowchart

FFAD permits node mobility in IoT networks. But whenever a node location is changed to an impossible distance between two successive communications, it will be flagged as the intruder node. Let the geographical location of a node n_x at time t be $\left(Lat_{n_{x_t}}, Long_{n_{x_t}}\right)$ and the previous location is $\left(Lat_{n_{x_{t-1}}}, Long_{n_{x_{t-1}}}\right)$, then the displacement D_{n_x} of the node n_x is calculated using the following equation.

$$D_{n_x} = \sqrt{\left(Lat_{n_{x_t}} - Lat_{n_{x_{t-1}}}\right)^2 + \left(Long_{n_{x_t}} - Long_{n_{x_{t-1}}}\right)^2}. \quad (6)$$

The Location anomaly severity label is assigned as follows.

$$L_{lo} = \begin{cases} High\ if\ D_{n_x} > D_{max_{n_x}} \\ Nada\ otherwwise \end{cases}, \quad (7)$$

where $D_{max_{n_x}}$ is the maximum possible displacement for the node n_x.

In FFAD, Any change in user privilege sets the Privilege anomaly severity label to high. Let $P_{n_{x_t}}$ be the privilege of the node n_x at a time t, the privilege anomaly severity label is determined as follows:

$$L_{pr} = \begin{cases} High\ if\ P_{n_{x_t}} \neq P_{n_{x_{t-1}}} \\ Nada\ otherwise \end{cases}, \quad (8)$$

where $P_{n_{x_{t-1}}}$ is the previous privilege of the node n_x.

A typical data packet header contains information such as header length, total length, source address, destination address, and time-to-live (TTL); FFAD uses a header flag set H with members $\{h_1, h_2, h_3, h_4, h_5\}$ for the corresponding header information. Any change in any of these information sets the corresponding flag to 1. The quantification$Q(H)$ of the overall set H is computed using Equation 9.

$$Q(H) = \frac{1}{5}\sum_{i=1}^{\overline{5}} h_i. \quad (9)$$

The header anomaly severity label L_{hdr} is determined by the equation:

$$L_{hdr} = \begin{cases} Nada\ if\ \dfrac{Q(H)}{5} = 0 \\ Low\ if\ 0 < \dfrac{Q(H)}{5} \leq {}^1\!/_4 \\ Medium\ if\ {}^1\!/_4 < \dfrac{Q(H)}{5} \leq {}^1\!/_2 \\ High\ otherwise \end{cases}. \quad (10)$$

Every IoT node is deployed to send one or more data from the sensor that can be categorized as numerical or text data. The payload dissection allows the FFAD module to monitor the data type during the transaction. If a change in the data type means the behavior of the node is suspicious. The Payload anomaly severity label L_{pl} is set to High if there is a change detected during the communication.

Any attempt to detect the possible connectivity ports in the base station between the communications will set the Port scanning anomaly severity label L_{ps} to High. Otherwise L_{ps} will be assigned to Nada. The tantamount procedure is followed to set the Ping sweep anomaly severity label L_{Pi}.

Connection duration is also an important parameter in detecting anomalies. Usually, a drastic increase in connection durations indicates a possibility of an intruder attack. Let $\lambda_{n_{x_{t-1}}}$ and $\lambda_{n_{x_t}}$ the two successive connection durations of the node n_x, the connection duration anomaly severity label is determined by the following equation:

$$L_{cd} = \begin{cases} High\ if\ \left(\lambda_{n_{x_t}} - \lambda_{n_{x_{t-1}}}\right) > {}^1\!/_4\, \lambda_{n_{x_{max}}}, \\ Nada\ otherwise \end{cases} \quad (11)$$

where $\lambda_{n_{x_{max}}}$ is the maximum permitted connection duration for the node n_x.

A change in the number of connections is also treated in the FFAD module since most of the IoT nodes are accustomed to using a single connection at a time. Let i_{n_x} and c_{n_x} be the initial and current number of connections of the node n_x, the number of connections anomaly sensitivity label L_{nc} is set to high wherever the value of c_{n_x} is greater than i_{n_x}.

The overall quantization of FFAD anomaly severity labels is computed using equation 12:

$$Q(L) = \frac{L_{tr,}+L_{bl}+L_{td}+L_{po}+L_{lo}+L_{pr}+L_{hdr}+L_{pl}+L_{ps}+L_{pi}+L_{cd}+L_{nc}}{\omega_{max} \times \text{number of parameters}}. \quad (12)$$

FFAD sets an Anomaly detection flag if there is more than a 25% chance of any combination of the above-discussed anomalies as by the following equation.

$$Anomaly = \begin{cases} TRUE\ if\ Q(L) > {}^1\!/_4. \\ FALSE\ otherwise \end{cases} \quad (13)$$

4.2. Legacy Naïve Bayes Attack Classifier (LNBAC). LNBAC is intended to classify a network anomaly into either of the following categories. They are Denial-of-Service, User-to-Root, Remote-to-Local, Probe and Normal. As per the standard Naïve Bayes algorithm is customized here to operate with 5 above-mentioned classifications and 12 features discussed in the FFAD module.

Algorithm 2. LNBAC Model Training

Input: Network Transaction Data Output: Trained Model
Step 1: Let Attack Classification Set $\alpha = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ Step 2: Let the selected feature set be $f = \{f_1, f_2 \dots f_{12}\}$ Step 3: Let $P(\alpha)$ be the prior probability Step 4: Let $P(f)$ be the Marginal Probability Step 5: Let $P(\alpha\|f)$ be the posterior probability of the class α for the feature f Step 6: Let $P(f\|\alpha)$ be the probability of the feature f given that the probability of the class α Step 7: $\forall i = 1 \rightarrow Attack\ classifications = 5 :: \forall j = 1 \rightarrow Number\ of\ features = 12 :=$ Step 8: Compute $P(\alpha_i)$ for the feature f_j Step 9: Compute the conditional probability $P(f_j\|\alpha_i)$ Step 8: Compute $P(\alpha\|f) = \frac{P(f\|\alpha)P(\alpha)}{P(f)}$ Step 9: return $P(\alpha\|f)$

The flow diagram for the LNBAC algorithm is given below (Figure 3). By this way, the attack classification is achieved by the LNBAC module.

Probe (Probing Attacks): These are attempts to gather information about a target network or system to identify potential vulnerabilities. Probing attacks are usually considered less severe because they are preliminary steps attackers take before launching more damaging attacks.

R2L (Remote-to-Local Attacks): These attacks involve unauthorized attempts to gain access to a local system from a remote machine. They are often considered more severe than probing attacks, as they can potentially lead to unauthorized access and data compromise.

U2R (User-to-Root Attacks): User-to-Root attacks are attempts by a user to gain administrative privileges on a system. These attacks are more serious because if successful, they can provide the attacker with full control over the compromised system, allowing them to install malicious software or manipulate data.

DoS (Denial-of-Service Attacks): Denial-of-Service attacks are among the most severe types of attacks. They involve overwhelming a system,

network, or service with excessive traffic or resource requests, rendering it unavailable to legitimate users. These attacks can lead to significant disruptions in services, financial losses, and reputational damage [18].

Normal network transaction refers to there is no evidence of any intruder attacks or network anomalies in the particular network communication attempt.

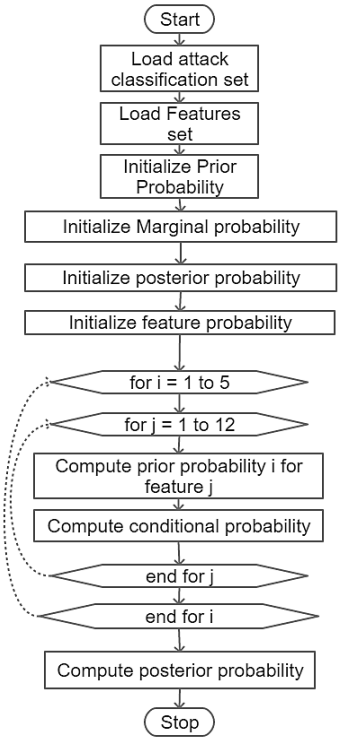

Fig. 3. LNBAC flowchart

4.3. Variable RSA Security Scheme (VRSS). The purpose of the VRSS module is to change the security strength dynamically based on the outputs of the FFAD and LNBAC modules. Instead of using a fixed security key size in RSA, the dynamic key selection VRSS will improve the security as well as the performance of the network by reducing the computational complexity when there is no or a little security anomaly detected. Whenever there is a hazard signal from FFAD and the classification of the attack from LNBAC, VRSS determines the required security key size circumspectly.

The base key size of VRSS is set to 256 bits, which can scale up to 1152 bits [19]. The key size for the RSA procedure is determined using the Anomaly severity index $Index_s$ and attack threat index $Index_t$.

The overall anomaly severity index $Index_s$ is determined as follows:

$$Index_s = \begin{cases} 1 \; if \; Q(L) < {}^1\!/_4 \\ 2 \; if \; {}^1\!/_4 \le Q(L) < {}^1\!/_2. \\ 3 \; if \; {}^1\!/_2 \le Q(L) < {}^3\!/_4 \\ 4 \; otherwise \end{cases} \quad (14)$$

The attack types Probe, R2L, U2R and DoS are assigned with the weights 2,3,4 and 5 respectively. The normal transaction type is assigned with the weight 1 to ensure basic security. That is the value of $Index_t$ will be 1, 2, 3, 4 and 5 for Normal, Probe, R2L, U2R and DoS respectively. The key size k is determined by using the following equation:

$$k = \left(\frac{1}{n_{sl}} \times (2^{n_{sl}} \times \; 2^{n_\tau})\right) \times (Index_s + Index_t), \quad (15)$$

where n_{sl} is the number of sensitivity labels, and n_t is the number of network transaction types.

Be like that the integration of FFAD, LNBAC and VRSS modules ensures fast and secure network communications in IoT network environments.

5. Experimental Setup. A computer with an i7 -8250U processor with 6MB Cache, 16GB DDR4 RAM and 1TB SSD storage is used to develop and evaluate the discussed procedures. Visual Studio IDE [20] is used to create the implementation solution, and C++ 20.0 [21] programming language is used to code the methodologies of ASORI. OPNET [22], which stands for "Optimized Network Engineering Tools", was a widely used software suite for network simulation, modeling, and performance analysis. The software allowed engineers, researchers, and network professionals to simulate and analyze various aspects of computer networks, telecommunications systems, and other communication technologies. OPNET provides several features such as Network Modeling, Simulation, Performance Analysis, Protocol Evaluation, and Resource monitoring/management. OPNET facilitated the testing of various network scenarios without the need for physical implementation, helping users identify potential issues before deployment. Users could analyze resource

utilization, bottlenecks, and optimization strategies within the network. OPNET was also used in academia to teach networking concepts and provide hands-on experience with network simulation.

The proposed IoT network Security method has extensive applications across diverse sectors, revolutionizing industries and enhancing efficiency, safety, and sustainability. From asset tracking and environmental monitoring to smart agriculture and energy management, IoT devices enable real-time data collection and analysis, empowering stakeholders to make informed decisions. In healthcare, IoT facilitates remote patient monitoring and personalized care, while in smart cities, it optimizes urban infrastructure and services for better quality of life. Retail and manufacturing benefit from IoT-driven automation and optimization, while home automation enhances convenience and energy efficiency for consumers. Industrial processes become more efficient and predictive with IoT-enabled automation, while safety and security are heightened through real-time monitoring and response capabilities. Overall, the broad spectrum of IoT applications underscores its transformative potential across various domains, shaping the future of technology-enabled innovation and connectivity.

6. Results and Analysis. Two different categories of results are obtained during the evaluation process. The first one is anomaly detection parameters such as Accuracy, Precision, Sensitivity, Specificity and F-Score. The second category is about network performance metrics such as Throughput, Latency, Jitter, End-to-End delay, Packet Delivery Ratio, Power consumption, and Security. Readings are taken for 1 real-world hour for every 6 minutes. Thus, there are 10 different timestamps used to log the parameters during the evaluation.

6.1. Accuracy. Anomaly detection accuracy is an important parameter in maintaining network stability. Since an anomaly can be an intruder attack, the anomaly detection process is a vital one in network security. It is calculated using the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). The accuracy is calculated using the formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}.$$

The ASORI method scored 99.135% of accuracy which is 1.2% higher than the nearest follower SIMA. The average accuracy of the proposed ASORI is 98.95% which is 1.4% higher than the second best SIMA method. The performance rank based on accuracy parameters is

ASORI, SIMA, ASDARS, EHDA, AIES and LCXMAC listed as the best. The measured accuracy values are provided in Table 2.

Table 2. Accuracy (%)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	96.37	91.41	95.57	97.61	91.64	98.82
2	96.13	91.72	95.15	97.56	91.37	99.08
3	96.33	91.68	95.49	97.23	91.51	99.03
4	96.66	91.40	95.68	97.72	91.43	98.86
5	96.22	91.86	95.38	97.93	91.43	99.01
6	96.61	91.18	95.61	97.25	91.44	98.79
7	96.54	91.36	95.52	97.50	91.65	99.04
8	96.76	91.06	95.28	97.36	91.16	99.13
9	96.65	91.14	95.52	97.54	91.76	98.97
10	96.37	91.28	95.67	97.76	91.31	98.78

6.2. Precision. Precision, in the context of data science and machine learning, is a metric that measures the accuracy of positive predictions made by a model. It is a concept often used in binary classification problems, where the goal is to classify instances into one of two classes: "positive" and "negative".

Precision is calculated using the formula $\frac{TP}{TP+FP}$. The computed Precision values are given in Table 3.

Table 3. Precision (%)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	95.69	92.34	96.93	96.45	92.47	98.05
2	95.14	92.78	96.1	96.92	92.01	98.46
3	95.28	92.56	96.64	96.22	92.35	98.35
4	95.49	92.69	96.78	96.53	92	98.23
5	95.13	92.81	96.12	96.97	92.66	98.22
6	95.47	92.09	96.74	96.12	92.68	98.18
7	95.90	92.35	96.99	96.47	92.81	98.3
8	95.54	92.01	96.56	96.35	92.27	98.53
9	95.87	92.22	96.07	96.23	92.89	98.32
10	95.38	92.48	96.68	96.98	92.49	98.06

As per the observations, ASORI scores the highest precision value of 98.53%, which is 1.54% higher than 96.99% of the closest performer EHDA. The precision average of ASORI is 98.27% during the overall experiment. The performance rank based on the average precision is

ASORI, EHDA, SIMA, ASDARSA, LCXMAC, and AIES listed as the best.

6.3. Sensitivity. Sensitivity refers to a metric used to evaluate the performance of a classification model, particularly in binary classification problems. It measures the ability of the model to correctly identify positive instances from the total actual positive instances. Sensitivity is also known as recall, hit rate, or true positive rate. Sensitivity is calculated using the formula $\frac{TP}{TP+FN}$. The observed sensitivity values are given in Table 4.

Table 4. Sensitivity (%)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	97.00	90.65	94.37	98.74	90.96	99.59
2	97.05	90.86	94.32	98.18	90.84	99.71
3	97.32	90.96	94.48	98.20	90.83	99.71
4	97.79	90.36	94.69	98.88	90.97	99.47
5	97.26	91.08	94.72	98.87	90.44	99.79
6	97.70	90.44	94.60	98.34	90.44	99.39
7	97.14	90.56	94.22	98.50	90.71	99.78
8	97.92	90.29	94.15	98.33	90.27	99.74
9	97.39	90.27	95.02	98.81	90.85	99.63
10	97.31	90.31	94.77	98.51	90.37	99.49

The experimental results show that ASORI work scored 99.78% anomaly sensitivity, which is higher than other methods. The average sensitivity of ASORI is 99.63% that shows the stability in terms of anomaly sensitivity.

6.4. Specificity. Specificity is one of the important metrics used to evaluate the performance of a binary classification model, particularly in scenarios where correctly identifying negative instances is crucial. Specificity measures the ability of the model to correctly identify negative instances from the total actual negative instances.

Specificity is calculated by $\frac{TN}{TN+FP}$. The measured specificity values for the proposed and existing methods are given in Table 5.

The ASORI method gained a specificity score of 98.55% which is 1.5% higher than the nearest achievement of 97.03% of the SIMA method. The performance rank based on the average specificity is ASORI, SIMA, EHDA, ASDARS, LCXMAC, and AIES with the scores 98.29%, 96.59%, 96.49%, 95.58%, 92.31% and 92.27% in their respective order listed as the best.

Table 5. Specificity (%)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	95.75	92.19	96.84	96.53	92.34	98.08
2	95.23	92.62	96.02	96.96	91.91	98.48
3	95.38	92.43	96.56	96.29	92.22	98.37
4	95.59	92.50	96.71	96.61	91.91	98.25
5	95.23	92.67	96.06	97.03	92.47	98.25
6	95.57	91.94	96.66	96.21	92.49	98.20
7	95.95	92.20	96.90	96.54	92.64	98.32
8	95.65	91.85	96.47	96.42	92.10	98.55
9	95.93	92.05	96.03	96.33	92.73	98.34
10	95.47	92.30	96.61	97.03	92.31	98.09

6.5. F-Score. The F-score, also known as the F1-score, is a metric used in classification tasks to assess the performance of a model, particularly in scenarios where class imbalance exists. It combines precision and recall into a single value and provides a balanced measure of a model's accuracy. The formula for F-Score calculation is $2 \times \frac{Precision \times Sensitivity}{Precision + Sensitivity}$. The F-Score values of the compared methods are given in Table 6.

Table 6. F-Score

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	0.9634	0.9149	0.9563	0.9758	0.9171	0.9882
2	0.9609	0.9181	0.9520	0.9754	0.9142	0.9908
3	0.9629	0.9175	0.9555	0.9720	0.9159	0.9902
4	0.9663	0.9151	0.9572	0.9769	0.9148	0.9885
5	0.9618	0.9194	0.9541	0.9791	0.9153	0.9900
6	0.9657	0.9126	0.9566	0.9722	0.9154	0.9878
7	0.9652	0.9144	0.9558	0.9747	0.9175	0.9903
8	0.9672	0.9114	0.9534	0.9733	0.9126	0.9913
9	0.9662	0.9123	0.9554	0.9750	0.9186	0.9897
10	0.9633	0.9138	0.9571	0.9774	0.9142	0.9877

The performance rank in terms of F-Score is ASORI, SIMA, ASDARS, EHDA, LCXMAC, and AIES the F-Score index averages 0.9894, 0.9752, 0.9643, 0.9554, 0.9156 and 0.9150.

The collective performance of the proposed ASORI method is perpetually higher than the compared methods in terms of Accuracy, Precision, Sensitivity, Specificity and F-Score. The experimental result evidently validates the enhanced performance of the ASORI method in Anomaly detection.

6.6. Throughput. Throughput refers to the rate at which data is successfully transmitted or received over a network. It is a measure of the

network's efficiency and capacity. The OPNET measures the throughput values during the simulation and the values are logged in Table 7.

Table 7. Throughput (kbps)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	27287	24274	27837	28688	24568	29303
2	27084	24039	27704	28905	24905	29407
3	27072	24082	27743	28917	24412	29475
4	27317	24418	27903	28933	24872	29637
5	27097	24260	28247	28908	25006	29642
6	27126	24281	28189	29051	24538	29743
7	27366	24043	27612	29029	24647	29332
8	27027	24330	27910	28524	24480	29450
9	27231	24541	28246	28543	24782	29558
10	27272	24528	27930	28504	24729	29589

As per the simulation results, the highest throughput of 29743 kbps is achieved by ASIRI during the 6th timestamp. The comparison graphs are given in Figure 4.

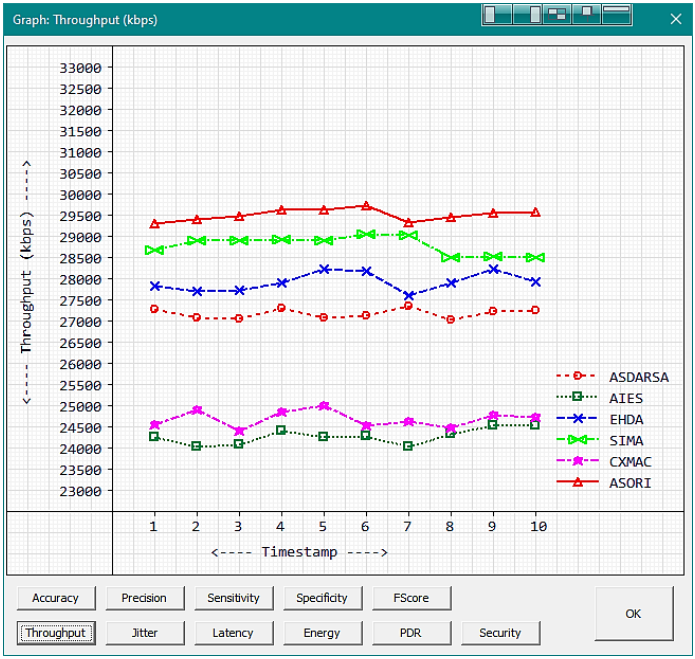

Fig. 4. Throughput graph

6.7. Latency. Latency refers to the delay or time lag that occurs when data packets travel from one point in a network to another. In general, Latency is measured in millisecond (ms) units. The observed Latency values during the simulation are given in Table 8. Latency is inversely proportional to the performance of the network architecture. Lower latency indicates the higher performance of the network.

The lowest latency 168mS is achieved by ASORI at the 6th timestamp during the simulation. The average latency of ASORI is about 180mS which is lesser than other compared methods (Figure 5).

Table 8. Latency (mS)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	299	460	269	224	444	191
2	310	473	277	212	426	186
3	310	470	275	212	453	182
4	297	452	266	211	428	173
5	309	461	248	212	421	173
6	307	460	251	205	446	168
7	295	472	282	206	440	190
8	313	457	266	233	449	183
9	302	446	248	232	433	177
10	300	446	265	234	436	176

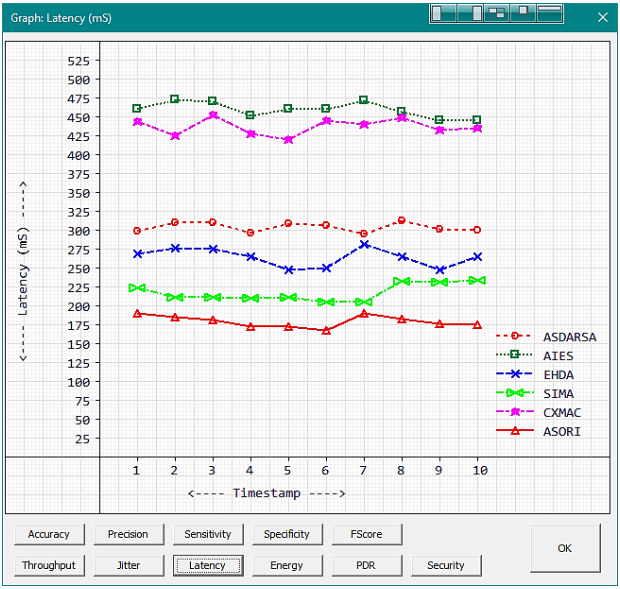

Fig. 5. Latency graph

6.8. Jitter. Jitter in the context of networking refers to the variation in the delay of packet delivery in a network. It is the irregular timing of data packets arriving at their destination. Higher jitter values lead to inconsistent network performance. The observed jitter values during the simulation are given in Table 9.

Table 9. Jitter (mS)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	102	150	93	80	145	70
2	105	154	95	76	140	68
3	105	153	95	76	148	67
4	101	148	92	76	141	64
5	105	151	87	76	139	64
6	104	150	88	74	146	63
7	101	154	97	74	144	69
8	106	149	92	82	147	67
9	103	146	87	82	142	66
10	102	146	92	83	143	65

The lowest jitter reading of 63mS is achieved by the ASORI method during the entire simulation. The jitter average of the ASORI method is 66mS which is lesser than other compared methods (Figure 6).

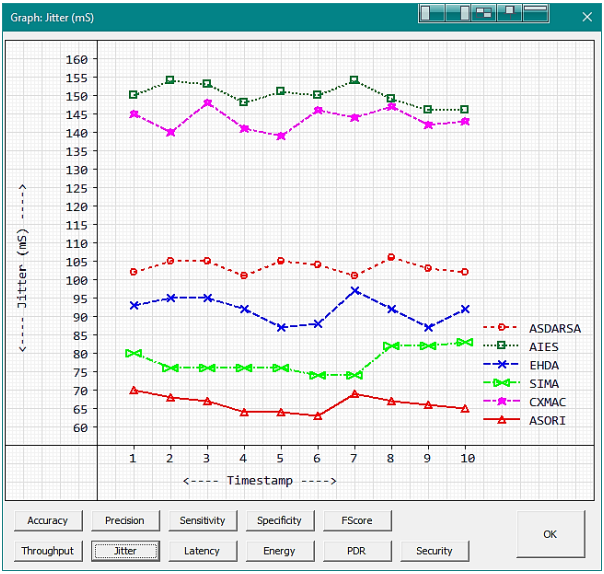

Fig. 6. Jitter graph

6.9. Energy. Energy efficiency is of paramount importance in Internet of Things (IoT) networks due to several key reasons such as power resource limitation of the nodes, Scalability of the network, and limited maintainability, Energy consumption is measured in millijoules units in a network. The energy readings during the simulation are given in Table 10.

Table 10. Energy (mJ)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	880	586	796	670	629	576
2	852	600	784	666	629	517
3	826	547	807	663	590	504
4	848	578	799	696	658	580
5	847	560	765	696	605	530
6	860	554	772	713	630	537
7	827	582	755	710	626	567
8	873	571	744	712	604	540
9	820	578	760	662	599	553
10	804	537	787	646	615	556

The experimental results show that the lowest energy consumption is achieved by the ASORI method during the complete simulation. ASORI is managed to operate with an average energy consumption of 546mJ. The comparison graph is given in Figure 7.

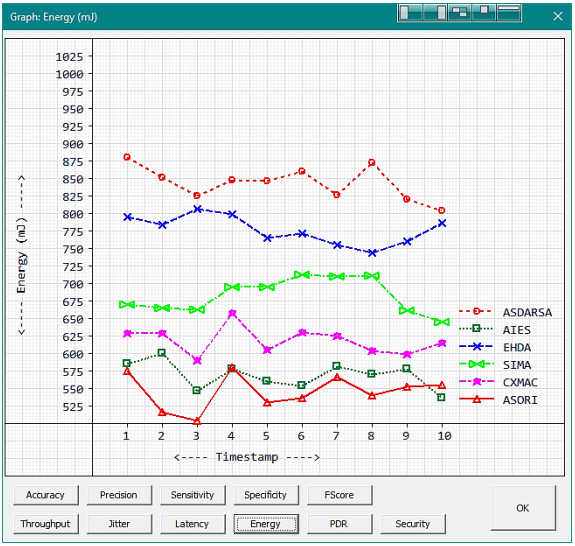

Fig. 7. Energy graph

6.10. Packet Delivery Ratio. Packet Delivery Ratio is a metric used to measure the reliability and performance of a communication network, particularly in wireless and packet-switched networks. It indicates the proportion of the successfully delivered packets compared to the total number of the sent packets. Table 11 is provided with the PDR values during the simulation.

PDR is a directly proportional network metric. Higher PDR indicates the higher performance of the network. The highest PDR 99.25% is achieved by the AOSRI method. The PDR average of the ASORI method is 99.17% which is also higher than the other compared methods (Figure 8).

Table 11. Packet Delivery Rate (%)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	98.43	97.42	98.61	98.90	97.52	99.10
2	98.36	97.35	98.57	98.97	97.64	99.14
3	98.36	97.36	98.58	98.97	97.47	99.16
4	98.44	97.47	98.63	98.98	97.62	99.21
5	98.37	97.42	98.75	98.97	97.67	99.21
6	98.38	97.43	98.73	99.02	97.51	99.25
7	98.46	97.35	98.54	99.01	97.55	99.11
8	98.34	97.44	98.64	98.84	97.49	99.15
9	98.41	97.51	98.75	98.85	97.59	99.19
10	98.42	97.51	98.64	98.83	97.58	99.20

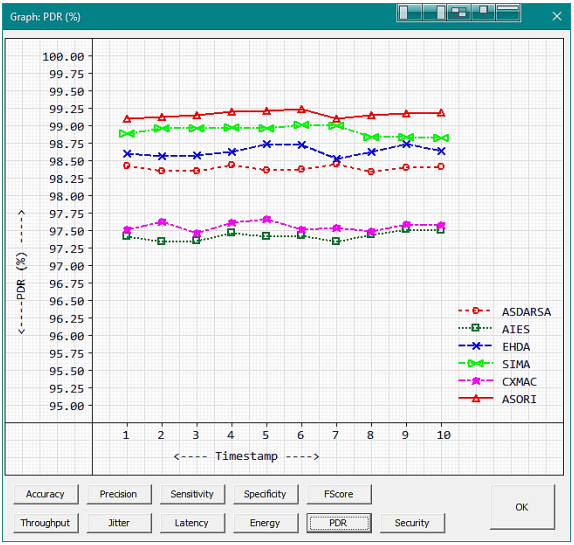

Fig. 8. Packet Delivery Ratio

6.11. Security. Security is crucial for Internet of Things (IoT) devices due to several significant reasons such as privacy protection, data integrity, device control, safety concerns, and long lifecycles. OPNET can determine the security level of the network environment under simulation by triggering a variety of intruder attacks. The measured Security scores of the examined methods are given in Table 12.

Table 12. Security Score (%)

Timestamp	ASDARSA	AIES	EHDA	SIMA	LCXMAC	ASORI
1	96.0000	91.5294	95.4118	97.3529	91.5882	99.5941
2	96.5882	91.7059	95.3529	97.2353	91.4706	99.5353
3	96.1176	91.0588	95.5882	97.2353	91.3529	99.3000
4	96.4118	91.2941	95.5882	97.1765	91.1176	99.5353
5	96.2941	91.2941	95.7647	97.7059	91.0000	99.6529
6	96.1765	91.7059	95.2941	97.4118	91.5882	99.4176
7	96.2941	91.2353	95.1765	97.7647	91.7059	99.4176
8	96.2353	91.8235	95.2941	97.8235	91.3529	99.5941
9	96.2941	91.7647	95.5294	97.7647	91.7059	99.3000
10	96.5294	91.7059	95.2941	97.7647	91.5294	99.4765

The comparison graph for security score is given in Figure 7.

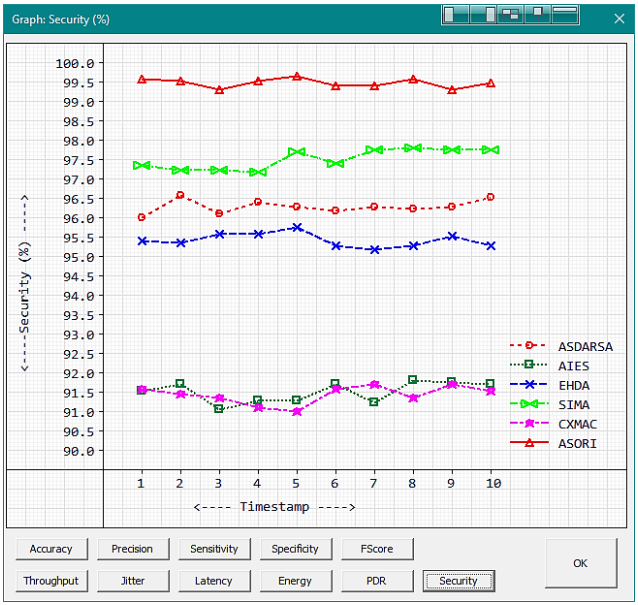

Fig. 9. Security score graph

The evaluation results show that the proposed ASORI method is the method that achieved the maximum security score of 99.66% at the 5th timestamp during the simulation. ASORI is capable of maintaining a security score of not less than 99.3%. The average security score of ASORI for the entire simulation is 99.48%. An improvement of 1.83% is achieved by the ASORI method than the security score of 97.82% of the nearest performing method SIMA.

7. Conclusion. The requirements can vary based on the specific use case, industry, and goals of the IoT deployment. A well-designed IoT architecture will carefully address these considerations to create a robust, secure, and efficient ecosystem which is attempted in this work. The experiments carried out during the evaluation process of the proposed ASORI method show that the work comes in handy with the expected advantages. The three novel modules FFAD, LNBAK and VRSS serve the purpose affirmatively. Improved IoT security is critical for safeguarding data privacy, protecting against unauthorized access, and ensuring the reliability of IoT devices and networks is addressed by the proposed method. Additionally, advancements in technologies like AI and blockchain offer innovative solutions for enhancing security and integrity. However, ongoing collaboration, innovation, and proactive measures are essential to stay ahead of evolving threats and maintain trust in IoT systems.

The advancements in terms of both network anomaly detection and overall network performance of the ASORI method put forward that the work can be encouraged for real-time IoT network environments. The dependency of RSA core is the limitation of ASORI work, and the incorporation of modern cryptography algorithms could be the future work.

Availability of Dataset: The work is intended to ensure dynamic IoT network security, thus dynamic network transactional simulation is used for evaluation.

Code Availability: The complete implementation source code is available on GitHub, the link will be provided on request.

References

1. Farrukh H., Ozmen M., Kerem Ors F. Celik Z. One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices. 2023 IEEE Symposium on Security and Privacy (SP). 2023. pp. 3026–3042. DOI: 10.1109/SP46215.2023.10179369.
2. Quy V., Hau N., Anh D., Ngoc L. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. Complex & Intelligent Systems. 2022. vol. 8. pp. 3805–3815. DOI: 10.1007/s40747-021-00582-9.
3. Rejeb A., Rejeb K., Simske S., Treiblmaier H., Zailani S. The big picture on the internet of things and the smart city: a review of what we know and what we need to know. Internet of Things. 2022. vol. 19. DOI: 10.1016/j.iot.2022.100565.

4. Inayat U., Zia M., Mahmood S., Khalid H., Benbouzid M. Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects. Electronics. 2022. vol. 11(9). DOI: 10.3390/electronics11091502.
5. Hatami M., Leinonen M., Chen Z., Pappas N., Codreanu M. On-Demand AoI Minimization in Resource-Constrained Cache-Enabled IoT Networks With Energy Harvesting Sensors. IEEE Transactions on Communications. 2022. vol. 70. no. 11. pp. 7446–7463. DOI: 10.1109/TCOMM.2022.3208873.
6. Nagaraju R, C V, J K, G M, Goyal SB, Verma C, Safirescu C, Mihaltan T. Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks. Energies. 2022. vol. 15(13). DOI: 10.3390/en15134777.
7. Fotohi R., Bari S., Yusefi M. Securing Wireless Sensor Networks against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. International Journal of Communication Systems. 2019. vol. 33(4). DOI: 10.1002/dac.4234.
8. Yang S.-K., Shiue Y.-M., Su Z.-Y., Liu I.-H., Liu C.-G. An Authentication Information Exchange Scheme in WSN for IoT Applications. IEEE Access. 2020. vol. 8. pp. 9728–9738. DOI: 10.1109/ACCESS.2020.2964815.
9. Ullah A., Said G., Sher M., Ning H. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Networking and Applications. 2020. vol. 13. pp. 163–174. DOI: 10.1007/s12083-019-00745-z.
10. Singh D., Kumar B., Singh S., Chand S. A Secure IoT-Based Mutual Authentication for Healthcare Applications in Wireless Sensor Networks Using ECC. International Journal of Healthcare Information Systems and Informatics. 2021. vol. 16. no. 2. pp. 21–48. DOI: 10.4018/IJHISI.20210401.oa2.
11. Ahmad A., Ullah A., Feng C., Khan M., Ashraf S., Adnan M., Nazir S., Ullah Khan H. Towards an Improved Energy Efficient and End-to-End Secure Protocol for IoT Healthcare Applications. Security and Communication Networks. 2020. vol. 2020. DOI: 10.1155/2020/8867792.
12. Nada A., Bayoumi M. Development of a constraint stabilization method of multibody systems based on fuzzy logic control. Multibody System Dynamics. 2024. vol. 61. pp. 233–265. DOI: 10.1007/s11044-023-09921-9.
13. Liu L., Xue D., Zhang S. General type industrial temperature system control based on fuzzy fractional-order PID controller. Complex and Intelligent Systems. 2023. vol. 9. pp. 2585–2597. DOI: 10.1007/s40747-021-00431-9.
14. Sivapriya N., Ravi T. Efficient Fuzzy based Multi-constraint Multicast Routing with Multi-criteria Enhanced Optimal Capacity–Delay Tradeoff. International Journal of Scientific & Technology Research. 2019. vol. 8(8). pp. 1468–1473.
15. Jasim A., Kashmar A. An Evaluation of RSA and a Modified SHA-3 for a New Design of Blockchain Technology. Artificial Intelligence for Smart Healthcare. EAI/Springer Innovations in Communication and Computing. Cham: Springer, 2023. pp. 477–489. DOI: 10.1007/978-3-031-23602-0_28.
16. Abid R., Iwendi C., Javed A., Rizwan M., Jalil Z., Anajemba J., Biamba C. An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. Personal and Ubiquitous Computing. 2023. vol. 27. pp. 1405–1418. DOI: 10.1007/s00779-021-01607-3.
17. Anushiya R., Lavanya V. A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of things. Measurement: Sensors. 2023. vol. 26. DOI: 10.1016/j.measen.2023.100700.
18. Roldan-Gomez J., Boubeta-Puig J., Carrillo-Mondejar J., Manuel Castelo Gomez J., del Rincon J. An automatic complex event processing rules generation system for the recognition of real-time IoT attack patterns. Engineering Applications of Artificial Intelligence. 2023. vol. 123. DOI: 10.1016/j.engappai.2023.106344.

19. Size considerations for public and private keys. Available at: https://www.ibm.com/docs/en/zos/2.3.0?topic=certificates-size-considerations-public-private-keys (accessed 26.01.2024).
20. Visual Studio 2022. Available at: https://visualstudio.microsoft.com/vs/ (accessed 10.02.2024).
21. Features of C++ 20. Available at: https://www.geeksforgeeks.org/features-of-c-20/ (accessed 04.02.2024).
22. OPNET Network Simulator. Available at: https://opnetprojects.com/opnet-network-simulator/ (accessed 16.14.2024).

Jenifer R. Rita — Research Scholar, PG & Research Department of Computer Science, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University. Research interests: computer science. The number of publications — 1. rita.jenifer@gmail.com; Cauvery Nagar Main Rd, Annamalai Nagar, 620018, Tiruchirappalli, Tamil Nadu, India; office phone: +91(431)275-1232.

Prakash V. Sinthu — Professor, PG & Research Department of Computer Science, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University. Research interests: computer science. The number of publications — 54. sinthujanita@gmail.com; Cauvery Nagar Main Rd, Annamalai Nagar, 620018, Tiruchirappalli, Tamil Nadu, India; office phone: +91(431)275-1232.

Acknowledgements. This research has been supported by the grant obtained under the scheme of Seed Money for Research projects from Cauvery College for Women (Autonomous), Tiruchirappalli.

УДК 004 **DOI** 10.15622/ia.23.5.6

Р. Дженифер, В.Д. Пракаш

АЛГОРИТМ RIVEST-SHAMIR-ADLEMAN, ОПТИМИЗИРОВАННЫЙ ДЛЯ ЗАЩИТЫ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ ОТ КОНКРЕТНЫХ АТАК

Дженифер Р., Пракаш В.Д. **Алгоритм Rivest-Shamir-Adleman, оптимизированный для защиты устройств Интернета вещей от конкретных атак.**

Аннотация. Устройства Интернета вещей играют важнейшую роль в современном мире во многих отношениях, поскольку они обеспечивают поддержку для зондирования окружающей среды, автоматизации и ответственного сохранения ресурсов. В «умном» мире повсеместное присутствие устройств Интернета вещей в повседневной жизни неизбежно. Широкое использование устройств Интернета вещей привлекает к себе любопытные взгляды злонамеренных хакеров. Несмотря на то, что существует несколько систем и протоколов безопасности, доступных для обычных беспроводных сетей, наблюдается необходимость в разработке современного механизма безопасности исключительно для сетевых сред Интернета вещей. Эта работа представляет улучшения безопасности сетей Интернета вещей. В ней собраны три специализированных способа для достижения более высоких показателей безопасности в сетевых средах Интернета вещей. Fast Fuzzy Anomaly Detector, Legacy Naïve Bayes Attack Classifiers и Variable Security Schemer of Rivest-Shamir-Adleman algorithm – это новые модули, представленные в этой работе, сокращенно ASORI. Уникальные преимущества встроенного механизма сертификации Интернета вещей и выбор динамической стратегии безопасности являются новшествами, представленными в данной работе. Модель ASORI была проверена с использованием промышленного стандартного симулятора сети OPNET для обеспечения улучшенной безопасности наряду с существенными улучшениями параметров производительности сети.

Ключевые слова: интернет вещей (IoT), сетевая безопасность, нечеткое обнаружение аномалий, наивная байесовская классификация, RSA.

Литература

1. Farrukh H., Ozmen M., Kerem Ors F. Celik Z. One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices. 2023 IEEE Symposium on Security and Privacy (SP). 2023. pp. 3026–3042. DOI: 10.1109/SP46215.2023.10179369.
2. Quy V., Hau N., Anh D., Ngoc L. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. Complex & Intelligent Systems. 2022. vol. 8. pp. 3805–3815. DOI: 10.1007/s40747-021-00582-9.
3. Rejeb A., Rejeb K., Simske S., Treiblmaier H., Zailani S. The big picture on the internet of things and the smart city: a review of what we know and what we need to know. Internet of Things. 2022. vol. 19. DOI: 10.1016/j.iot.2022.100565.
4. Inayat U., Zia M., Mahmood S., Khalid H., Benbouzid M. Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects. Electronics. 2022. vol. 11(9). DOI: 10.3390/electronics11091502.
5. Hatami M., Leinonen M., Chen Z., Pappas N., Codreanu M. On-Demand AoI Minimization in Resource-Constrained Cache-Enabled IoT Networks With Energy Harvesting Sensors. IEEE Transactions on Communications. 2022. vol. 70. no. 11. pp. 7446–7463. DOI: 10.1109/TCOMM.2022.3208873.

6. Nagaraju R, C V, J K, G M, Goyal SB, Verma C, Safirescu C, Mihaltan T. Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks. Energies. 2022. vol. 15(13). DOI: 10.3390/en15134777.
7. Fotohi R., Bari S., Yusefi M. Securing Wireless Sensor Networks against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. International Journal of Communication Systems. 2019. vol. 33(4). DOI: 10.1002/dac.4234.
8. Yang S.-K., Shiue Y.-M., Su Z.-Y., Liu I.-H., Liu C.-G. An Authentication Information Exchange Scheme in WSN for IoT Applications. IEEE Access. 2020. vol. 8. pp. 9728–9738. DOI: 10.1109/ACCESS.2020.2964815.
9. Ullah A., Said G., Sher M., Ning H. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Networking and Applications. 2020. vol. 13. pp. 163–174. DOI: 10.1007/s12083-019-00745-z.
10. Singh D., Kumar B., Singh S., Chand S. A Secure IoT-Based Mutual Authentication for Healthcare Applications in Wireless Sensor Networks Using ECC. International Journal of Healthcare Information Systems and Informatics. 2021. vol. 16. no. 2. pp. 21–48. DOI: 10.4018/IJHISI.20210401.oa2.
11. Ahmad A., Ullah A., Feng C., Khan M., Ashraf S., Adnan M., Nazir S., Ullah Khan H. Towards an Improved Energy Efficient and End-to-End Secure Protocol for IoT Healthcare Applications. Security and Communication Networks. 2020. vol. 2020. DOI: 10.1155/2020/8867792.
12. Nada A., Bayoumi M. Development of a constraint stabilization method of multibody systems based on fuzzy logic control. Multibody System Dynamics. 2024. vol. 61. pp. 233–265. DOI: 10.1007/s11044-023-09921-9.
13. Liu L., Xue D., Zhang S. General type industrial temperature system control based on fuzzy fractional-order PID controller. Complex and Intelligent Systems. 2023. vol. 9. pp. 2585–2597. DOI: 10.1007/s40747-021-00431-9.
14. Sivapriya N., Ravi T. Efficient Fuzzy based Multi-constraint Multicast Routing with Multi-criteria Enhanced Optimal Capacity–Delay Tradeoff. International Journal of Scientific & Technology Research. 2019. vol. 8(8). pp. 1468–1473.
15. Jasim A., Kashmar A. An Evaluation of RSA and a Modified SHA-3 for a New Design of Blockchain Technology. Artificial Intelligence for Smart Healthcare. EAI/Springer Innovations in Communication and Computing. Cham: Springer, 2023. pp. 477–489. DOI: 10.1007/978-3-031-23602-0_28.
16. Abid R., Iwendi C., Javed A., Rizwan M., Jalil Z., Anajemba J., Biamba C. An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. Personal and Ubiquitous Computing. 2023. vol. 27. pp. 1405–1418. DOI: 10.1007/s00779-021-01607-3.
17. Anushiya R., Lavanya V. A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of things. Measurement: Sensors. 2023. vol. 26. DOI: 10.1016/j.measen.2023.100700.
18. Roldan-Gomez J., Boubeta-Puig J., Carrillo-Mondejar J., Manuel Castelo Gomez J., del Rincon J. An automatic complex event processing rules generation system for the recognition of real-time IoT attack patterns. Engineering Applications of Artificial Intelligence. 2023. vol. 123. DOI: 10.1016/j.engappai.2023.106344.
19. Size considerations for public and private keys. Available at: https://www.ibm.com/docs/en/zos/2.3.0?topic=certificates-size-considerations-public-private-keys (accessed 26.01.2024).
20. Visual Studio 2022. Available at: https://visualstudio.microsoft.com/vs/ (accessed 10.02.2024).
21. Features of C++ 20. Available at: https://www.geeksforgeeks.org/features-of-c-20/ (accessed 04.02.2024).

22. OPNET Network Simulator. Available at: https://opnetprojects.com/opnet-network-simulator/ (accessed 16.14.2024).

Дженифер Р. Рита — научный сотрудник, научно-исследовательский отдел компьютерных наук, Женский колледж Кавери, Университет Бхаратидасан. Область научных интересов: компьютерные науки. Число научных публикаций — 1. rita.jenifer@gmail.com; Главная улица Кавери-Нагар, Аннамалай-Нагар, 620018, Тируччираппалли, Тамил Наду, Индия; р.т.: +91(431)275-1232.

Пракаш В. Синту Джанита — профессор, научно-исследовательский отдел компьютерных наук, Женский колледж Кавери, Университет Бхаратидасан. Область научных интересов: компьютерные науки. Число научных публикаций — 54. sinthujanita@gmail.com; Главная улица Кавери-Нагар, Аннамалай-Нагар, 620018, Тируччираппалли, Тамил Наду, Индия; р.т.: +91(431)275-1232.

Поддержка исследований. Исследование было поддержано грантом, полученным в рамках программы начального финансирования исследовательских проектов от Женского колледжа Кавери, Тируччираппалли.