ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20240822001935
Original scientific paper

A Comprehensive Integrated Security Model with Advanced Access Control for Enhancing WSN Computing in IoT Frameworks

Navaneethan S.*, Arun A.*

Abstract: Wireless Sensor Network (WSN) Computing has emerged as a pivotal intermediary process addressing latency challenges inherent in Cloud-oriented Internet of Things (IoT) services. However, this advancement brings forth significant security and privacy concerns exacerbated by the proliferation of network nodes and the vast volumes of real-time data generated within IoT frameworks. To mitigate these issues, this research proposes an Integrated Security Model with Advanced Access Control (ISM-AAC) Mechanism. The ISM-AAC integrates Functional Encryption (FE) and Role-Based Access Control (RBAC) to fortify communication security. The model employs a comprehensive approach encompassing Access Control Processes, Integrated Encryption Processes, and Re-Encryption Processes to enhance data confidentiality and integrity. The detailed framework includes phases such as system initialization, user management, and access permission administration, ensuring robust security throughout data transactions. Evaluation of the model's efficacy is conducted based on various security metrics pertinent to WSN computing environments. This study contributes to the advancement of secure computing in IoT by proposing a sophisticated ISM-AAC framework that not only addresses current security challenges but also anticipates future threats in the landscape of WSN computing. The findings underscore the model's effectiveness in safeguarding sensitive IoT data and lay the groundwork for future enhancements in IoT security protocols.

Keywords: Advanced Access Control (AAC); functional encryption; Internet of Things (IoT); security model; Wireless Sensor Networks (WSN)

1 INTRODUCTION

In recent scenario of computing, WSN Computing is the new computing paradigm that is developed for supplementing cloud computing. It helps to enhance the process of internet computation and complexity because of the increasing new methods and solutions. The requirement of data processing and storage is also increased. For handling the rising demands, web architecture is developed [1]. The centralization of services in cloud paradigm reduces the time effectiveness and the mobility support through which there is a latency created between the request and the service providing. For solving Sensor Sensor computing is developed [2]. It enables Access Point (AP) hosting to the end devices. It allows many software and services to execute closely for processing the data. Here, the fog nodes own several centralized interfaces for providing global synchronization. Though the Sensor computing development is recent, this model has been combined by the advanced cloud and data models. The model is developed based on the concept of distributed computing and includes data delivery network; makes the delivery easier for simpler process. However, the features of Sensor computing are distinguished from cloud based on the end users, data processing, computation and services [4].

Though there are several advantages in cloud, the fog model has some security issues. Those issues develop new paradigms of security based confrontations that affects the data processing and the overall network. The influence of the security issues can affect the communication flow between the edge devices in cloud, edge and Sensor computing. Hence, securing the fog model and creating advanced data protection includes incorporation of authentication, access control, data confidentiality and integrity. Many research works are developed for many models for solving the security problems in Sensor, which are not considerably efficient and robust in providing security over communication.

Sensor computing solves the centralization issue of cloud and in the proposed model, the security requirement of Fog is effectively analyzed and a model is developed. In order to ensure the privacy of the user data, advanced cryptographic methods are used. Moreover, it is explicit that the access control of the user data of each used is to be ensured by the computing model. For supporting the fine-grained data access control and privacy maintenance of user data, here, Functional Encryption is incorporated. The flow and computations of functional encryption are used here, and the private key and the cipher text are linked with the attribute set and the decryption process is carried out, if and only if the key features are matched. Here, for instance, in processing the patient health data in secure manner, the Health Department is considered as the Central Authority (CA) for the process of FE. Particularly, when the used with definite attribute is connected to the model, the CA generates a key for that input. With that, the complete process of FE is carried out.

Additionally, the model is combined with Role based Access Control (RBAC) for solving the present access control methods. Here, a new model called Integrated Security Model with Advanced Access Control (ISM-AAC) Mechanism is proposed. And, in the following section, the computations, formal definitions, model framing explanations are given. Moreover, the proposed model is effectively adapted for the access control policies that are dynamically updated. And also the model efficiency and performances are improved by utilizing FE and RBAC. Based on the methods and evaluations of access control process, the model shows its efficacy in preserving access control and security with higher rate of model performance by the integration of cryptographic process.

The remainder of this paper is arranged as follows; Section 2 mentions the related works in handling security challenges in computing paradigms. The preliminaries of the proposed model are presented in Section 3. The proposed model explanation with computations and diagram is given in Section 4. The results and discussions are provided with the implementation of explanations and comparisons in Section 5, and the model performances are

also evaluated. Finally, the model is concluded and the remarks are given in Section 6 with some additional ideas for future work.

2 RELATED WORKS

Attribute Based Encryption (ABE) is used in many security models for access control in Fog Computing. Fuzzy Identity-based Encryption model is developed in [5], in which the attribute based encryption model is used. Two-attribute based encryption models are derived based on the access control methods [6], as, Key Policy Attribute Based Encryption (KPABE) [7] Cipher-text Policy Attribute Based Encryption (CPABE) [8]

Using CPABE [9], the data security model is developed, in which the private and public keys are given for read and write access. Moreover, the model uses the key distribution model for efficient key management to provide access control over the communications. However, the key management process is complicated, when the access permissions are becoming large. Further, a bounded access control model is proposed in [10], in which, CPABE is used for fine-grained access control. The authors of [11] developed an Anonymous Access Control Model for securing the used privacy over communication. In [12], a cloud security access control model is proposed for user authentication and privacy preserving in Cloud framework.

For handling the side channel attack, efficient leakage resilient cryptographic models are discussed in [13] and [14]. Among all methods, Continual Memory Leakage model is concluded as the best, in which the lifetime is divided in time slots. At the end of each slot, the model's private state is updated. The amount of leaked data in each slot is bounded and the total leakage in processing is unbounded. Moreover, the model incorporated many cryptographic techniques such as digital signatures [15], ABE [16], Identity Based Encryption (IBE) [17], Multi-party Computation [18] and so on. Adaptive Resource Access Control using RBAC Model is proposed in [19]. The model is adaptive and effective on dynamic environmental changes in cloud computing. RBAC is combined with trust management model in [20], as DRBAC. The model provides access permissions to the roles and PKI based security is used with certification process for processing private data. Moreover, the model has been implemented with multi-domain processing.

Ontology-based Access Control model is proposed in [21] that defines the difference between the allowed access control for service providers and consumers. Further, in [22], negotiation policy has been used for framing the access control model and an UCON-based cloud model is derived. In the same way, a risk management model has been proposed in [23] and an access control process is designed accordingly. The aforementioned models used trust management model for providing access control over data processing. For secure data access, in [24], a formal verification model has been developed. The model is involved in managing security between the fog edges and nodes. For that, Shibboleth protocol has been used and it is concluded that the model has not considered the threat types. The flexible IoT based model is given for cloud-fog communication in handling the security of the communication model. Additionally, the model developed resource-aware security for the smart devices. The results of the model showed that the pre-shared keys are effective in providing privacy and the alternative methods are determined for secure communications. Furthermore, a hybrid access control model has been developed for hierarchical security processing with minimal complexities. Still, there are some computational complexities in the model. RBAC is combined with IBE for security over the cloud files. As the RBAC is a static model, the model is effective in dynamic environments for processing with the access control policies. For solving the issues presented in the discussed works in cloud and fog, the paper is involved in developing a novel model.

3 PRELIMINARIES

An integrated security model with advanced access control mechanisms in a Wireless Sensor Network (WSN) typically aims to ensure the confidentiality, integrity, and availability of data collected by the sensors. The main goals and processes involved in such a security model include confidentiality, integrity, availability, access control, key management event intrusion detection and prevention, secure routing, secure Data aggregation, Physical Layer Security, and Security Monitoring and Logging. Packet Loss, Latency, Bandwidth Limitations, Network Congestion and Security Threats were the issues faced in the data transmission model.

Here, random factor is considered as 'r' which is given as $r < -R$ uniform finite set. And, (m) denotes the set as [1, 2, 3, , m] and 'F' is given as the group, 'f' $\in f$ and:

$$B = (b_1, b_2, b_3, ..., b_n) \in z_n \tag{1}$$

and the elements are termed as:

$$b = (fk_1, fk_2, ..., fk_n) \tag{2}$$

Component-based multiplication vectors are considered. The predicate function is defined as $R = \{R_b\} r$, with an invariable constant factor $a \in m$, where R_b: $X_b \times Y_b \rightarrow \{0, 1\}$ maps the feature pair between the X_b and Y_b key spaces. Here, b" denotes the index parameter, indicating that R_b belongs to R.

The first input of b represents the domain rate of the function R_b. Additionally, R_m is denoted as R_b, which is domain-transferable if, for r that divides M, the projection map is given as follows.

$$f_1: X_m \rightarrow x_r, f_2: y_m\, y \rightarrow r \tag{3}$$

such that for all x belongs to X_m & Y belongs to y_m if $R_m(x, y = 1)$ then, $R_r(f_1(x), f_2(y)) = 1$ and if $R_m(x, y = 0)$ then $R_r(f_1(x), f_2(y)) = 0$.

The predicate function of the functional encryption R is a combination of four operations, Set_Up, Key Generation, Encryption and Decryption.

Set_Up Phase:

Setup(a, b) = (pubKey, MSeckey) in which the input security factor is denoted as, ' ' for the index factor, 'b', Output is given as MSeckey as Master Secret Key and pubKey as public key.

Key Generation:
$Key\_Gen(X, MSecKey, PubKey) \rightarrow SecKey$ (4)

in which the key generation takes *MSeckey*, *pubKey* as input and creates the output, Secke for '*X*'.

Encryption:
$Enc(Y, D, PubKey)$---- $\rightarrow Ciptext$ (5)

The inputs include an attribute, message '*D*,' and PubKey, while the output is derived as *cipText*, which denotes the cipher text.

Decryption:
$Dec\ (MSeckey, cipText \rightarrow D)$ (6)

It takes the secret key and cipher text as inputs and generates the data as output.

In the Role-Based Access Control (RBAC) concept, the model includes system initialization, user registration, role management, data management, and data access.

System Initialization: The access control process operates during system initialization using Functional Encryption (FE) to generate key attributes. Subsequently, an FE-based key is generated for the user (U) as Genkey FE (u) → Enckey, and the signature key is generated as Genkey FE (u) → Seckey for authentication.

User Registration: The new users are required to register themselves with their encryption and secret key with the model. Here, the key transmissions are carried out through the secure channel

Role Management: Through this, the role is included in the generated key as '*r*' which is given as:

userrole U,r,EncUFe(*Seckey*, *Enckey*)
SignUFe (7)

Data Management: For each data function used by the role '*r*,' (*r*, function operation) is assigned to the admin and created before being uploaded to the cloud in the following pattern.

(*Admin, r*(*function operation*),
EnergyuFeU, *SignUeFe*) (8)

Data Access: When the user is getting access for reading the data file, 'd*f*"

$df(u, r) = (r, df, read) \in Admin$ (9)

Further, the tuples of relevant users are downloaded, the signatures are verified, file decription is carried out with the obtained key.

4 PROPOSED MODEL

In this section, the complete workflow and computations of the proposed Integrated Security Model with Advanced Access Control (ISM-AAC) Mechanism are explained in detail. Fig. 2 illustrates the components of the security model and its functional flow.

In the proposed model, the application is designed to operate with a cloud storage provider, which is considered untrusted. To ensure data confidentiality, users must be authenticated and authorized before accessing shared data. Additionally, the model includes third parties such as access control administrators, storage providers, and users, whose roles are outlined below.

By performing key verification, the access control mechanism generates a new symmetric key for the tuples, enabling secure communication over the network.

A. Elements of the Model.

I. Access control Admins.

The element is responsible for managing the access control operations of the outsourced data. The operations include the key generation FE and updating the access control policies. Additionally, the element is also responsible for addition, allocation, deletion and revocation of users and roles.

II. Storage Provider.

The responsibility of the storage provider is to manage the data storage requirements of users. Here, access control policies are also stored to ensure data security. The provider is assumed to be untrusted, making it essential to secure the stored content by allowing only authorized individuals to access the data. It must also be ensured that unauthorized users cannot access the data, the content remains unchanged, and the access policies remain secure.

Users.

Users utilize the storage services, which are controlled by the Access Control Admins. They must register and use keys to ensure model security. Users are granted access to upload and download data.

Functions of the Proposed Model.

The Role based access control based on the functional encryption in Fog can be presented with a tuple representation with seven functions, which is given as follows:

FE-RBAC=
= (*setup, user*, *accessPermission*, *role,userAllocation*,
permissionAllocation, *read/write*) (10)

Setup_ Phase.

This phase is for system initialization, the security factor 'n' is given as input, which produces a general factor of functional encryption model and a master key and produces FE based secret key and decryption key for the administrator.

User (add_user, del_user).

This includes the addition and deletion of users. For performing addition and deletion operations, the user id is used for generating the keys and further, the user deletion is performed by revoking the user from the model. After revocation, the users are not able to access the data that is stored.

Access permission (Add (fn,fc)).

This function is responsible for adding and deleting permissions and includes the file name along with its corresponding contents. When an addition request is received, the data file is encrypted and shared over the cloud. When a deletion request is activated, the specific file is removed from the model.

Role (Addition(*r*), deletion(*r*)).

This function performs two operations: adding and deleting roles. When an addition command is received with

the role ID, the role is added to the access control model, and a decryption and signature key is generated for data access. When a deletion command is received, the specified role is removed from the model.

User Allocation (Assign, Revoke).

This function performs the user allocation and revocation process. The user and the role id is given as the input for the function, which performs the resource assignment and revocation based on the received command, respectively. '*nm*,'

Permission Allocation (Assign, Revoke).

The access permission for the outsourced data is performed by this function. For inputs, the name of the data file, role and the access privilege are considered. With that, the permission assignment and revocation are processed.

Read/Write (data file).

This function performs the reading and writing operations on the data file. The user id and the file name are given as the inputs. For writing operation, the data file is updated with the new content and further it is uploaded on to the storage.

User allocation and revocation is performed with the function assign_user(r_user) and revoke user(r,user), respectively. And the pseudocode for the process is presented in Tab. 1.

Table 1 Pseudo code for allocation and revocation of users

```
Begin
For user allocation
   Perform Tuple Download and perform sign
    verification using signkey
   Do
    Signature verification
    Build Tuple
    Upload to role manager
    Stores the received tuple on to the storage
   End do
  End for
For user revocation
   Generate new decryption and signature key with FE
   Generate new tuple for data can perform all roles
   Perform tuple download
   Upload to role manager
   Delete tuples
  Generate new keys
   Build a new tuple and upload on to role manager
End For
End
```

Permission Allocation and Revocation.

Here, the permission allocation and revocation is performed with the following functions,

i. Assign parameters.
ii. Revoke parameters.

And the steps involved in the function are provided below,

i. Check whether the role has permission for data reading and requires write access.
ii. Perform tuple download.
iii. Perform signature verification.
iv. Frame new tuple with update access permission.
v. Upload on to role manager.

When the role does not have any access rights over the file,

i. new tuple with required access permission is developed.
ii. upload on to role manager.

Then, for performing revocation process,

For removing the write access only, the following operation is performed.

i. Perform key verification.
ii. When both accesses are revoked, delete all
iii. Generate new symmetric key.
iv. Frame new tuples.
v. Update the data onto the storage.

B. Reading Data File and Writing Data File

For file reading, the tuple is downloaded initially, as, and the signature verification is done using the decryption key of user, the tuple '*Y*' is generated.

Here, key is used for file decryption, and the data file is obtained. Then users are allowed to write access and then uploaded. When the user is allocated with the write access, for role '*r*' and the tuple is generated.

After downloading the tuple, signature verification is done. Following, decryption operations are carried out. New tuple is generated and updated on to the role manager. Additionally, the old tuple with that file name is deleted.

5 RESULTS AND DISCUSSION

For analyzing the efficiency of the proposed model, the implementations are done and tested with Cloud Sim tool. Here, the proposed model is mainly designed for providing access control over the shared data, in fog computing environment. The parameters such as user names, roles, versions, data files and tuple sets are considered for evaluation. Moreover, the obtained results are compared with KPABE, IBE and RBAC. The results are focused on measuring the time and the computational complexity between models along with storage efficiencies.

Table 2 Time consumption access analysis vs file size

Models	32	64	128	256	512	1024
ISM-AAC	129.11	178	400	500	600	663.24
IBE	191.27	243.4	469.58	543.22	630.25	669.46
RBAC	165.45	291.21	434.67	582.43	656.55	708.67
K PABE	208.49	252.48	486.79	551.82	625.94	743.1

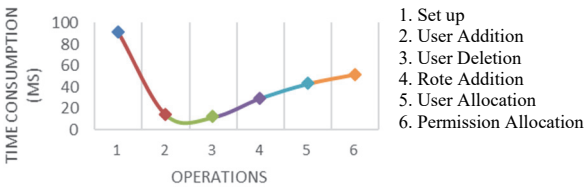

Figure 1 Time consumption analysis for basic operations

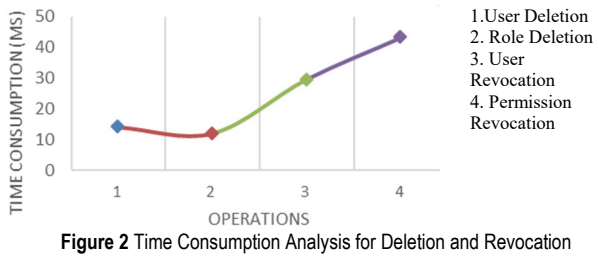

Figure 2 Time Consumption Analysis for Deletion and Revocation

Fig. 1 presents the graph for the time based evaluations for the major six operations such as setup, user addition and deletion, role addition, user allocation and permission allocation. And Fig. 2 provides the graph for the computed

results of the operations, user deletion, role deletion, user revocation and permission revocation.

The main objective of the proposed model is to provide access control over the shared data, which are effectively achieved with the aforementioned operations.

Table 3 Values obtained for Read & Write Access

Models	32	64	128	256	512	1024
ISM-AAC-R	129.11	178	400	500	600	663.24
IBE-R	191.27	243.4	469.58	543.22	630.25	669.46
RBAC-R	165.45	291.21	434.67	582.43	656.55	708.67
K PABE-R	208.49	252.48	486.79	551.82	625.94	743.1
ISM-AAC-W	130.07	186.49	421.28	508.79	604.42	678.06
IBE-W	208.97	226.18	477.7	526	603.95	686.67
RBAC-W	191.27	261.09	552.3	582.9	656.07	712.97
K PABE-W	213.27	291.21	565.21	569.52	630.25	721.58

Time consumption for processing with the data size is measured and provided in Tab. 2 and the corresponding graph is portrayed in Fig. 3. The results are compared with the existing models. It is observed from the graph that the proposed model takes 411.725 ms in average for processing, the data file size as 32, 64, 128, 256,612, 1024, KB. The graph clearly shows that the proposed model achieves a lower time consumption rate compared to the other models.

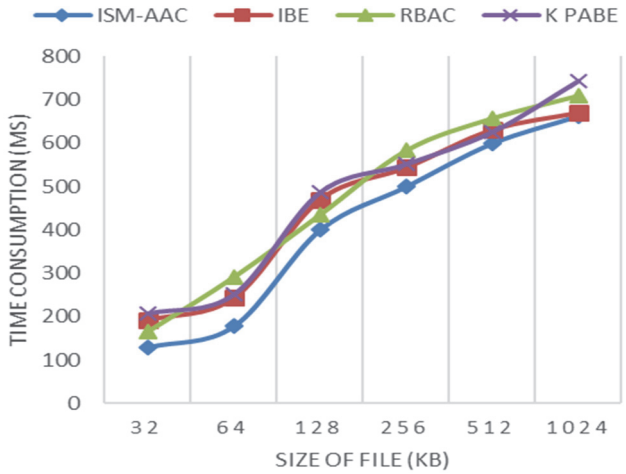

Figure 3 Time consumption vs file size

When considering the data access in fog computing, the analysis should be carried out of read and write access for the data shared. The evaluations are carried out for all the compared models for the time taken to perform the read and write operations. This can be processed after the user gets the access permission on shared data. The obtained values are given in the following Tab. 3 and the comparison graph is given in Fig. 4. It is explicit from the graph that the proposed work takes minimal time for the process.

Table 4 Time complexity vs operations

Models	1	2	3	4	5
ISM-AAC	33.17	43.42	52.65	62.42	83.5
IBE	45.03	60.21	74.27	80.82	85.11
RBAC	64.56	78.62	73.2	81.36	90
KPABE	58.61	82.97	88.92	76.47	86.24

Other time complexity based evaluations based on the proposed model operations are carried out and the results are provided in Fig. 5. For the major operation of the proposed work, the time taken is evidenced as minimal and the values are given in Tab. 3.

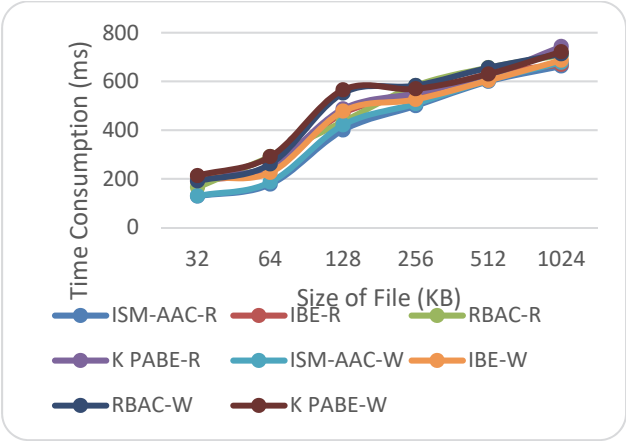

Figure 4 Time consumption comparison for read and write access

In the proposed model, in terms of providing access control over the shared data, the model integrates the efficiencies of Functional Encryption operations and RBAC. In ISM-AAC, by the model effectiveness, the computational complexity is considerably less than other works. And the obtained results are provided in Tab. 5 and the graph is depicted in Fig. 6.

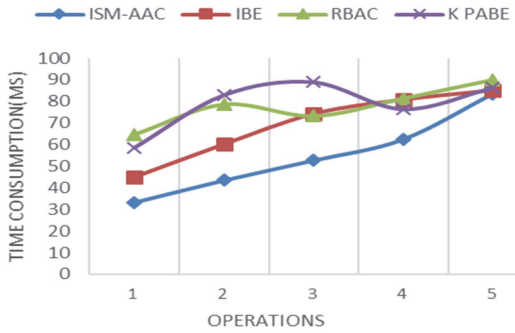

Figure 5 Comparisons between models for time complexity

Table 5 Results obtained for computational complexity

Models	32	64	128	256	512	1024
ISM-AAC	21.23	25.34	29.71	35.68	41.66	44.89
IBE	27	34.07	38.97	51.46	53.08	62.28
RBAC	25.4	36.76	42.74	57.44	62.88	72.09
K PABE	32.99	43.87	47.64	65.57	69.4	81.35

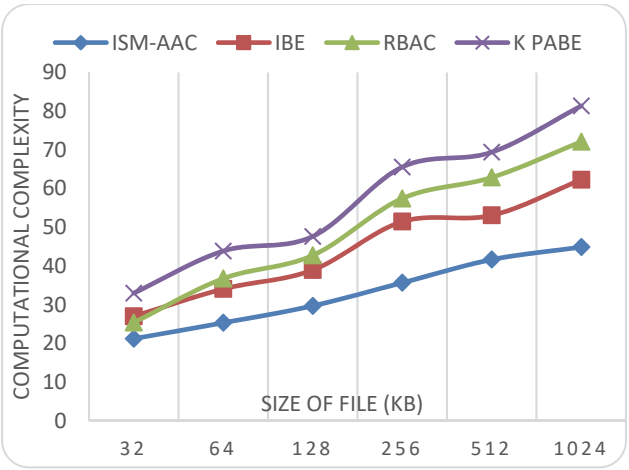

Figure 6 Computational complexity vs file size

6 CONCLUSION AND FUTURE WORK

This paper presents the Integrated Security Model with Advanced Access Control (ISM-AAC), which utilizes Functional Encryption (FE) within Fog Computing. The model allows for dynamic changes in access privileges and defines a detailed construction involving tuple generation, key generation, and access control operations for reading and writing shared data. By combining FE with Role-Based Access Control (RBAC), the model enhances performance and efficiency, demonstrating superiority over existing approaches in terms of computation and time complexity. Future work may focus on ensuring data integrity with advanced cryptographic standards and implementing the model in real-time environments for functional security testing. The performance impact of the model varies based on the encryption algorithms used; larger systems with numerous devices and users may face resource-intensive evaluations of access control policies. While Attribute-Based Access Control (ABAC) offers flexibility, it can introduce additional complexity. The ISM-AAC framework is designed to anticipate future IoT security threats by integrating adaptive security measures and machine learning algorithms for behavioral analysis and anomaly detection. This proactive approach helps identify potential threats before they are manifested. The framework allows for adaptive access control, enabling automatic adjustments of permissions based on unusual device behavior. By incorporating artificial intelligence and machine learning, the model facilitates real-time data analysis, ensuring robust and resilient security in an evolving IoT landscape.

7 REFERENCES

[1] Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2024). A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal, 14*, 3440-3450. https://doi.org/10.1109/JSYST.2020.2970167

[2] Tandale, U., Momin, B., & Seetharam, D. P. (2024). An empirical study of application layer protocols for IoT. *Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2447-2451.

[3] Kumar, R., Kumar, P., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. (2023). PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Transactions on Network Science and Engineering, 8*, 2326-2341. https://doi.org/10.1109/TNSE.2021.3089435

[4] Gopinath, S., Vinoth Kumar, K., & Elayaraja, P. (2020). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.12.1096

[5] Balakrishnan, S. & Vinoth Kumar, K. (2023). Hybrid Sine-Cosine Black Widow Spider Optimization based Route Selection Protocol for Multihop Communication in IoT Assisted WSN. *Technical Gazette, 3*0(4), 1265-1273. https://doi.org/10.17559/TV-20230201000306

[6] Ovsthus, A. A. K. S. K. & Kristensen, L. M. (2014). An industrial perspective on wireless sensor networks-A survey of requirements, protocols, and challenges. *IEEE Communications Surveys & Tutorials, 16*, 1391-1412. https://doi.org/10.1109/SURV.2014.012114.00058

[7] Vinoth Kumar, K. & Rajakani, V. (2024). Modeling of Intrusion Detection System using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment. *Brazilian Archives of Biology and Technology, 67*, e24231010. https://doi.org/10.1590/1678-4324-2024231010

[8] Muneeba, N., Javed, A. R., Tariq, M. A., Asim, M., & Baker, T. (2022). Feature engineering and deep learning-based intrusion detection framework for securing edge IoT. *Journal of Supercomputing.*

[9] Vinoth Kumar, K. & Balakrishnan, S. (2023). Multi-objective Sand Piper Optimization Based Clustering with Multihop Routing Technique for IoT Assisted WSN. *Brazilian Archives of Biology and Technology, 66*, e23220866. https://doi.org/10.1590/1678-4324-2023220866.

[10] Osterrieder, P., Budde, L., & Friedli, T. (2020). The smart factory as a key construct of Industry 4.0: A systematic literature review. *International Journal of Production Economics, 221*, 107476. https://doi.org/10.1016/j.ijpe.2019.08.011

[11] Devesh, M., Kant, A. K., Suchit, Y. R., Tanuja, P., & Kumar, S. N. (2020). Fruition of CPS and IoT in context of Industry 4.0. *Intelligent Communication, Control and Devices*, 367-375. Springer. https://doi.org/10.1007/978-981-13-8618-3_39

[12] Vinoth Kumar, K. & Thiruppathi, M. (2023). Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog Assisted Wireless Sensor Network. *Acta Montanistica Slovaca, 28*(2), 243-251. https://doi.org/10.46544/AMS.v28i2.18

[13] Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems, 131*, 209-226. https://doi.org/10.1016/j.future.2022.01.017

[14] Rajakani, V. & Vinoth Kumar, K. (2023). Barnacles Mating Optimizer with Hopfield Neural Network Based Intrusion Detection in Internet of Things Environment. *Technical Gazette, 30*(6), 1750-1760. https://doi.org/10.17559/TV-20230414000533

[15] Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J. P. C., & Park, Y. (2020). Intrusion detection protocols in wireless sensor networks integrated to the Internet of Things deployment: Survey and future challenges. *IEEE Access, 8*, 3343–-3363. https://doi.org/10.1109/ACCESS.2019.2962829

[16] Ponni, R., JayaSankar, T., & Vinoth Kumar, K. (2023). Investigations on Underwater Acoustic Sensor Networks Framework for RLS Enabled LoRa Networks in Disaster Management Applications. *Journal of Information Science and Engineering, 39*(2), 517-526.

[17] Granjal, J., Monteiro, E., & Silva, J. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*, 1294-1312. https://doi.org/10.1109/COMST.2015.2388550

[18] Sharma, V., Patel, R. B., Bhadauria, H. S., & Prasad, D. (2016). Deployment schemes in wireless sensor network to achieve blanket coverage in large-scale open area: A review. *Egyptian Informatics Journal, 17*, 45-56. https://doi.org/10.1016/j.eij.2016.06.001

[19] Wang, W., Qiu, C., Yin, Z., Srivastava, G., Gadekallu, T. R., Alsolami, F., & Su, C. (2021). Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3117762

[20] Javed, A. R., Beg, M. O., Asim, M., Baker, T., & Al-Bayatti, A. H. (2020). Alphalogger: Detecting motion-based side-channel attack using smartphone keystrokes. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-01770-0

[21] Azmoodeh, A., Dehghantanha, E., & Choo, K. K. R. (2019). Robust malware detection for Internet of (battlefield) Things devices using deep eigenspace learning. *IEEE Transactions on Sustainable Computing, 4*, 88-95. https://doi.org/10.1109/TSUSC.2018.2809665

[22] Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in Industry 4.0. *IEEE Internet of Things Journal, 8*, 2300-2317. https://doi.org/10.1109/JIOT.2020.3025916

[23] Ghayvat, H., Mukhopadhyay, S., Gui, X., & Suryadevara, N. (2015). WSN- and IoT-based smart homes and their extension to intelligent building. *Sensors Journal, 15*, 10350-10379. https://doi.org/10.3390/s150510350

[24] Faheem, M. (2019). Bio-inspired routing protocol for WSN-based smart grid applications in the context of Industry 4.0. *Transactions on Emerging Telecommunications Technologies, 30*, 1-24. https://doi.org/10.1002/ett.3675

Contact information:

Navaneethan S., Research Scholar
(Corresponding author)
Department of Networking & Communications,
School of Computing,
SRM Institute of Science and Technology,
SRM Nagar, Kattan Kulathur, Tamilnadu, India-603203
E-mai: ns2066srmist@gmail.com

Arun A., Associate Professor
(Corresponding author)
Department of Networking & Communications,
School of Computing,
Faculty of Engineering & Technology,
SRM Institute of Science and Technology Kattan
Kulathur, Tamilnadu, India-603203
E-mail: aruna2@srmist.edu.in