Journal Of Technology

Issn No:1012-3407

Scopus And Ugc Approved Journal

Website:https://technologyjournal.net/

ELSEVIER

Certificate of Publication

Article Id:JOT/1076

Published a paper entitled

A Theoretical Study of IoT Data Security Through the Integration of Machine Learning, Artificial Intelligence and Blockchain Technology

Author by

Dr Ujwal A. Lanjewar

Binzani Mahila Mahavidyalaya, Nagpur, MS. (India).

Published in Volume 13 Issue 8 2023

UGC APPROVED

Google Scholar Crossref doi Academia.edu CiteFactor

Editor-In-Chief
Andreas Thor

A Theoretical Study of IoT Data Security Through the Integration of Machine Learning, Artificial Intelligence and Blockchain Technology

Ms. Priyanka S. Yengantwar (Chandawar)[#1], Dr Ujwal A. Lanjewar[#2], Dr S. J. Sharma[#3]

[#1]*Assistant Professor, Department of Computer Science, Dr. S. C. Gulhane Prerna College of Commerce, Science, and Arts, Nagpur, MS. (India)*

[#2]*Professor, & Principal, Department of Computer Science, Binzani Mahila Mahavidyalaya, Nagpur, MS. (India)*

[#3]*Head of Department of Electronics & Computer Science Rashtrasant Tukadoji Maharaj Nagpur University, Research Centre, Nagpur, MS. (India)*

Abstract The **Internet of Things (IoT) is one of the most rapidly used technologies in the last decade in various applications. The smart devices are connected wireless or wired for communication, processing, computing, and monitoring different real-time operations. The devices are heterogeneous with low memory and less processing power. The implementation of IoT applications comes with challenges like security and privacy because traditional-based security protocols do not match IoT devices. In this paper, in the first section, the author describes an overview of the IoT technology. The primary security issues like confidentiality, Integrity, Availability, and layer-wise issues are identified. Then the author studied the three primary technologies for addressing the security issue in IoT that is Machine learning (ML), Artificial intelligence (AI), and Blockchain. In the end, security issues were solved by the integration of ML, AI, and Blockchain. This paper proposes a comprehensive approach to fortify IoT security by harnessing the synergy of Machine Learning (ML), Artificial Intelligence (AI), and Blockchain technology.**

Keywords- Internet of Things, Machine learning, Artificial intelligence and Blockchain

I. INTRODUCTION

The Internet of Things (IoT) is a network of smart devices that share information over the Internet. The smart devices are used to deploy in a different environment to fetch the information, and some events are triggered. As per CISCO's estimate, the active IoT devices will be 50 billion at the end of 2020. The number of IoT devices is rapidly increasing day by day. The data generated by the IoT devices is huge. In traditional IoT, architecture there are three types of layers available namely physical, network, and application layers. In the physical layer, devices are embedded with technology in which they sense the atmosphere and are also able to connect IoT devices. For example, in smart hospitals, patients can monitor an emergency through sensors and corresponding computing devices. As we know sensors and IoT devices have less computation power and are heterogeneous. Implementation of IoT leads to lots of challenges such as standardization, interoperability, data storage, processing, trust management, identity, confidentiality, integrity, availability, security, and privacy. Later on, these challenges related to surveys work on IoT security.

The main objective of this paper is to find out the security and privacy challenges that are available in IoT applications. It has also identified some unfold technology that can address security issues present in the system.

A. IoT Infrastructure

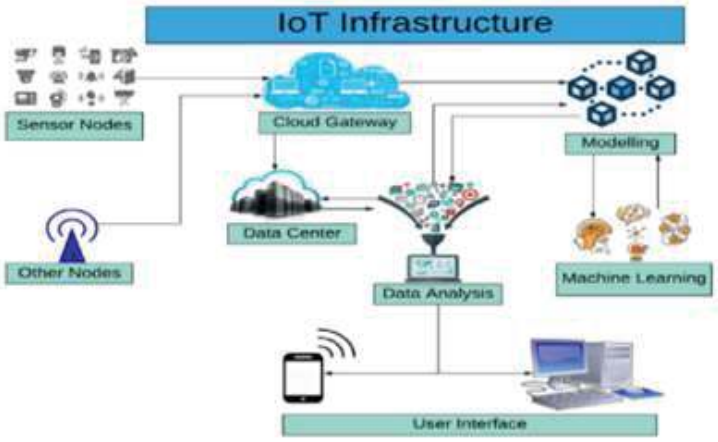

Figure 1. Internet of Things Infrastructure

IoT application contains several smart devices that collect, process, compute, and communicate with different smart devices. It has three layers physical, network, and application layer. As shown in Fig. 1 IoT infrastructure consists of sensors integrated with some emerging technologies, which are based on either IoT-cloud or IoT-fog-cloud. The architecture of IoT may be centralized, distributed, or decentralized structure. The most challenging issue in the IoT application is processing and computing in real time. We know that cloud computing provides vast storage and assures security to the data. But now most of the real-time monitoring IoT application demands processing and computing at the edge of the network. When it is done at the edge using fog nodes, it becomes more vulnerable to attackers. During analytic data. an advanced technique like Machine Learning is used to make the IoT system more intelligent and independent in making a decision. The different smart devices are connected to make an application using some standard protocols. The data interoperability [1] in IoT works using an intelligent algorithm.

Table 1 shows four layers in IoT infrastructure, their standard protocol name, and possible security attacks in respective layers.

Table 1

Protocols and attacks on the IoT layer

Layer	**Protocol Name**	**Possible security attack**
Application	MQTT, CoAP, REST, AMQP	Repudiation Attack, DDoS Attack, HTTP Flood Attack, SQL Injection Attack, Cross-Site Scripting, Parameter Tampering, Slowloris Attack
Transport	TCP, UDP, DCCP, SCTP, RSVP, QUIC	SYN Flood, Smruf Attack, Injection Attack, Opt-ack Attack
Network	CLNS, DDP, EIGRP, ICMP, IGMP, IPsec, IPv4, IPv6, OSPF, RIM	IP Address Spoofing, DoS Attack, Black Hole Attack, Worm Hole Attack, Consumption Attack
Physical	DSL, ISDN, IDA, USB, Bluetooth, CAN, Ethernet	Access Control Attack, Physical Damage or Destruction, Disconnection of Physical Links

B. Machine Learning and Artificial Intelligence: Machine Learning and Artificial Intelligence offer their expertise to the identification of anomalous behaviors, predictive threat analytics, and real-time monitoring. These technologies enable the creation of dynamic behavioral patterns, facilitating the prompt detection of deviations from the norm. AI-driven authentication methods, including biometric recognition and natural language processing, bolster access control mechanisms, thereby enhancing overall IoT device security.

C. Blockchain technology: Blockchain technology, known for its immutable and decentralized nature, forms a robust foundation for the proposed security paradigm. By immutably storing IoT data and

transactional records, Blockchain ensures data integrity and offers an auditable trail of events. Additionally, the introduction of autonomous identities and smart contracts empowers devices to establish their authenticity and autonomously execute predefined security protocols.

II. LITERATURE REVIEW

Reference Paper	Year	Research Work
Jing et al. [2]	**2014**	This paper stated the security issues of the three layers of IoT and its corresponding solutions.
Ngu et al. [3]	**2016**	The author described the IoT middleware-based architecture adaptability and security issues in the IoT system.
Mosenia et al. [4]	**2016**	The author explained the reference model and security threads present on the edge of the network and it also addresses the possible solutions.
Lin et al. [5]	**2017**	This paper describes the IoT and Cyber-Physical System (CPS) integration with the survey of the security and privacy issues.
Yang et al. [6]	**2017**	In this survey, the four-layer computing integration based on IOT application is explained in this survey paper.
Alaba et al. [7]	**2017**	In this paper, the authors investigate the state of the art of security and privacy issues on IoT applications and systems. It also reviewed the authentication protocol in the IT system and challenging security issues in the four-layer architecture based on the IoT application.
Grammatikis et al. [8]	**2018**	In this paper, the author provides a detailed study of the IOT security layer-wise. The suitable countermeasures and the potential threats model are discussed in detail.
Das et al. [9]	**2018**	In this paper, the author investigates the security and threat model in IT applications. This paper also describes some of the issues in IT system like authentication, trust, management, and access control, and some solution approach was also addressed.
Di Martino et al .[10]	**2018**	In this paper, the different standard architectures of IoT systems and the current solution approach in terms of security and interoperability are explained.
Hassija et al. [11]	**2019**	In this paper, the author reviewed the security and three in IoT application, whereas different solution approach using machine learning, fog computing, edge computing, and Blockchain was proposed.
Proposed Paper	**2023**	In this paper, the author initially identified the necessary infrastructure protocol of the IoT system. Then the security issues are identified in the IoT model. Some emerging techniques that can be used to solve the security issues in IoT have been identified. After a rigorous survey, the author found that machine learning, Blockchain, and artificial intelligence are the current solution approaches to solving the security issues in IoT.

III. SECURITY ISSUE ADDRESS USING MACHINE LEARNING (ML) AND ARTIFICIAL INTELLIGENCE (AI)

Machine learning is a technique to perform intelligent computation. The model always needs to be designed and tested using various learning methods. For example, predicting a fire in a kitchen or any industrial area and alarm to prevent the fire. This could be possible if machine learning technologies are used in IoT applications. Also, it needs to address the security issue present in the IoT system to make the system tamper-proof. Whereas AI could help IoT huge volumes, unstructured data, and heterogeneous data to compute in real-time, which makes the system realistic. IoT security with Machine Learning (ML) and Artificial Intelligence (AI). Here's how each technology can contribute:

A. *Anomaly Detection:* ML and AI algorithms can analyze patterns of normal behavior for IoT devices and networks. Any deviations from these patterns can be flagged as potential security breaches, enabling quick responses to mitigate risks.

B. *Behavioral Analysis:* By continuously learning and adapting to device behavior, ML algorithms can identify evolving threats and adapt security protocols accordingly.

C. *Predictive Analytics:* ML can predict potential security threats based on historical data, helping organizations take proactive measures to prevent breaches.

D. *Real-time Monitoring:* AI-driven systems can monitor IoT networks in real-time, detecting and responding to security incidents as they occur.

E. *Advanced Authentication:* AI can power advanced authentication mechanisms like biometric recognition, voice recognition, or facial recognition for access control.

a. *Natural Language Processing (NLP):* NLP can be used to analyze and understand the context of communication between IoT devices, identifying suspicious or unauthorized interactions.

IV. SECURITY ISSUE ADDRESS USING BLOCKCHAIN TECHNOLOGY

Blockchain technology is a decentralized and distributed network where each block is connected to others in some way. The message is broadcast in the Blockchain network. A block consists of lots of trusted transactions and their associated attributes. Following are the contributions of AI in IoT Security.

A. *Immutable Data Storage:* Blockchain's decentralized and tamper-proof nature ensures that data collected from IoT devices remains secure and unalterable, maintaining data integrity.

B. *Secure Transactions:* Blockchain facilitates secure and verifiable transactions between IoT devices, reducing the risk of unauthorized access or data manipulation.

C. *Decentralized Identity Management:* Blockchain can enable self-sovereign identities for IoT devices, enhancing authentication and access control while reducing the risk of identity theft.

D. *Audit Trails:* All transactions and changes are recorded on the blockchain, creating an audit trail that helps trace the origin of security breaches and unauthorized activities.

E. *Smart Contracts:* Smart contracts can automate security protocols and responses. For instance, if an anomaly is detected, a smart contract can trigger predefined actions to isolate or shut down compromised devices.

F. *Consensus Mechanisms:* Blockchain's consensus algorithms ensure that changes to the system are agreed upon by a majority of participants, preventing unauthorized modifications.

V. INTEGRATION OF TECHNOLOGIES MACHINE LEARNING WITH ARTIFICIAL INTELLIGENCE

ML and AI can enhance the accuracy of anomaly detection, behavioral analysis, and predictive analytics in the context of IoT security. Blockchain can provide a secure and transparent data storage layer for ML and AI models, ensuring the integrity of algorithms and results. Combined, these

technologies can create a holistic security framework where IoT data is collected securely, analyzed for threats, and stored in a tamper-proof manner.

VI. CHALLENGES AND CONSIDERATIONS

A. *Resource Constraints:* IoT devices often have limited computational resources. ML and AI algorithms must be optimized to run efficiently on these devices.

B. *Scalability:* As IoT networks grow, ensuring that ML, AI, and blockchain solutions can scale to handle the increased load is essential.

C. *Data Privacy:* While ML and AI require substantial data for training, data privacy concerns must be addressed. Blockchain's privacy features (e.g., zero-knowledge proofs) can help in this aspect.

D. *Regulatory Compliance:* Depending on the industry and location, there may be regulations governing the use of AI, ML, and blockchain in IoT security. Compliance is crucial to avoid legal issues.

Incorporating ML, AI, and blockchain into IoT security strategies can create a robust and adaptive defense against evolving threats. However, implementation requires careful planning, collaboration between experts in various domains, and ongoing monitoring to ensure the system's effectiveness and resilience.

CONCLUSION

The Internet of Things (IoT) in recent times attracted lots of attention to the research community as well as the industry sector. The IoT devices are manufactured in large numbers which already cross the total world population. These smart devices are connected to different applications for capturing information from the environment. The IoT devices are resource-constrained, so devices are vulnerable to attackers. Security and privacy issues are important for IoT applications.

In this paper, the authors first study in-depth the IoT infrastructure also various security challenges that exist in it. Secondly, the authors have found that some research has already been done on various technologies like Machine learning, Artificial intelligence, and Blockchain technology, which are capable of addressing the existing security issues. So, in detail, a study has been made on three technologies machine learning, artificial intelligence, and Blockchain technology, and their integration with IoT. Security is an important issue that needs to be addressed. In this paper, the authors outline emerging technologies like ML, AI, and Blockchain integrated with IoT to make the system more secure.

REFERENCES

[1] Nawaratne, Rashmika, et al. "Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments." Future Generation Computer Systems, vol. 86, 2018, pp. 421-432.

[2] Jing, Qi, et al. "Security of the Internet of Things: Perspectives and challenges." Wireless Networks, vol. 20, 2014, pp. 2481-2501.

[3] Ngu, H. Anne, et al. "IoT middleware: A survey on issues and enabling technologies." IEEE Internet of Things Journal vol 4, no.1 2016, pp.1-20.

[4] Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of the security of internet-of-things." IEEE Transactions on Emerging Topics in Computing vol 5, no.4, 2016, pp. 586-602.

[5] Lin, Jie, et al. "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal, vol.4, no.5,2017, pp. 1125-1142.

[6] Yang, Yuchen, et al. "A survey on security and privacy issues in Internet-of-Things." IEEE Internet of Things Journal vol.4., no.5, 2017, pp. 1250-1258.

[7] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks, vol.54, no.15, 2010, pp. 2787-2805.

[8] Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." Internet of Things, vol 5, 2019, pp. 41-70.

[9] Das, Ashok Kumar, Sherali Zeadally, and Debiao He. "Taxonomy and analysis of security protocols for Internet of

Things." Future Generation Computer Systems, vol.89, 2018, pp. 110-125.

[10] Di Martino, Beniamino, et al. "Internet of things reference architectures, security and interoperability: A survey." Internet of Things Vol.1 ***(2018):*** *pp. 99-112.*

[11] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 ***(2019)****: pp.82721-82743.*

Journal Of Technology

Issn No:1012-3407

Scopus And Ugc Approved Journal

Website:https://technologyjournal.net/

ELSEVIER

Certificate of Publication

Article Id:JOT/1072

Published a paper entitled

Elevating Weather Prediction for Recurrent Neural Networks and Long Short-Term Memory Models

Author by

Dr Ujwal A. Lanjewar

Binzani Mahila Mahavidyalaya, Nagpur, MS. (India).

Published in Volume 13 Issue 8 2023

UGC APPROVED

Google Scholar Crossref doi Academia.edu CiteFactor Academic Scientific Journals

Editor-In-Chief
Andreas Thor

Elevating Weather Prediction for Recurrent Neural Networks and Long Short-Term Memory Models

Ms. Rupali B. Surve[#1], Dr Ujwal A. Lanjewar[#2], Dr S. J. Sharma[#3]

[#1]*Assistant Professor, Department of Computer Science, Dr. S. C. Gulhane Prerna College of Commerce, Science, and Arts, Nagpur, MS. (India)*

[#2]*Professor, & Principal, Department of Computer Science, Binzani Mahila Mahavidyalaya, Nagpur, MS. (India)*

[#3]*Head of Department of Electronics & Computer Science Rashtrasant Tukadoji Maharaj Nagpur University, Research Centre, Nagpur, MS. (India)*

Abstract- ***The ability to anticipate the weather is essential in many industries, including disaster relief, transportation, and renewable energy. For making decisions, weather forecasting must be precise and timely. Numerical weather prediction models that replicate intricate atmospheric processes are the foundation of traditional meteorological approaches. Recurrent neural networks and long short-term memory models, in particular, have shown their capacity to improve weather prediction accuracy by identifying complicated temporal patterns in historical weather data in recent years. This study, which uses RNNs and LSTM models to improve weather prediction, is presented in this paper. The purpose of the study is to show that these models are more accurate than traditional numerical weather prediction models at forecasting weather variables like temperature, humidity, rain, and wind speed.***

Keywords- Recurrent Neural Network, Long Short-Term Memory, NWP Model, Deep Learning, Machine Learning, Time Series Prediction

I. INTRODUCTION

Accurate weather forecasting plays a crucial role in various applications across multiple sectors due to its impact on safety, planning, decision-making, and resource management. Weather forecasts support various scientific studies, including climate research, atmospheric studies, and environmental monitoring. Accurate predictions contribute to a better understanding of Earth's climate and weather patterns. Weather prediction has always been a complex challenge due to the intricate and nonlinear nature of atmospheric phenomena. Weather forecasting has a long history of development, starting with traditional methods and evolving into more sophisticated approaches, including early attempts with machine learning [1].

II. TRADITIONAL METHODS FOR WEATHER PRECISION

1) *Empirical observations: The earliest weather forecasts were based on the precise measurement of atmospheric parameters like temperature, humidity, wind speed, and precipitation. Meteorologists working at weather stations made these observations.*

2) *Numerical Weather Prediction (NWP):* In the middle of the 20th century, the invention of computers made it possible to mimic the behavior of the atmosphere using intricate mathematical models. To anticipate how atmospheric conditions will vary over time, NWP entails splitting the atmosphere into a grid of points and utilizing mathematical equations. This methodology remains an essential component of contemporary weather forecasting.

3) *Synoptic Meteorology:* By examining large-scale weather elements including pressure systems, fronts, and jet streams, meteorologists investigate synoptic-scale weather patterns. Meteorologists can forecast the future weather in particular places by studying these patterns [1].

III. EARLY ATTEMPTS WITH MACHINE LEARNING

A. *Pattern Recognition:* Researchers started using machine learning methods like neural networks to forecast the weather in the 1980s and 1990s. In these early experiments, pattern identification was the main focus, and the model was trained to link particular patterns of atmospheric variables with particular weather outcomes [2].

B. *Neural Networks:* Complex correlations between numerous meteorological factors and their effects on weather patterns were learned using neural networks. However, the low computational power at the time and the short datasets hindered these early attempts [3].

C. *Hybrid Models:* Machine learning methods and conventional NWP models have begun to be combined by researchers. They employed machine learning, for instance, to enhance parameterizations in NWP models, which are the approximate representations of small-scale processes that the models can't directly express due to their low resolution [4].

D. *Data Assimilation:* Data assimilation, in which observable data and model predictions are integrated to produce more precise initial conditions for NWP models, is another area where machine learning has found use. Long-range forecasts often contain inaccuracies that can compound over time. Data assimilation helps lessen these flaws [5].

E. *Ensemble Forecasting:* Machine learning techniques were employed to develop ensemble forecasting systems. These systems generate multiple forecasts using slightly different initial conditions to account for the inherent uncertainty in weather predictions [5].

F. *Advancements in Deep Learning:* As computing power increased and deep learning gained popularity, more advanced neural network architectures like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) were applied to weather forecasting tasks. These architectures excel at capturing spatial and temporal dependencies in data [6].

Recurrent neural networks (RNNs) and Long Short-Term Memory (LSTM) models in particular have demonstrated promising results in increasing the accuracy of weather forecasting. Due to their specialization in working with sequential data, RNNs and LSTMs are excellent choices for time-series data like weather observations. Traditional numerical weather prediction models, which simulate atmospheric processes using intricate physical equations, frequently have trouble capturing all the nuances and uncertainties of actual weather patterns. Machine learning can help with this. To learn patterns from historical weather data and use these patterns to predict future weather conditions, RNNs, and LSTMs must be able to capture temporal dependencies in data. A sophisticated form of RNN known as LSTM models uses memory cells and gating methods to get around the vanishing gradient issue. They are particularly suited for time series forecasting applications like weather prediction because they can capture both short-term and long-term relationships in sequential data [1].

IV. LITERATURE REVIEW

Hochreiter, S, et al introduced the Long Short-Term Memory (LSTM) architecture, which addressed the vanishing gradient problem in training RNNs and enabled better capture of long-range dependencies in sequences in this fundamental paper [7].

Gallicchio, C., et al. explored the application of Echo State Networks (a type of RNN) for time series prediction, showing the potential of RNNs in capturing complex temporal patterns [8].

Benjamin Lindemann et al focus on the application of LSTM networks in anomaly detection. It discusses various LSTM-based models and their use in detecting anomalies in different domains [9].

Greff, K., Srivastava, et al explore the evolution of LSTM architectures and various modifications that have been proposed over the years. It provides insights into how LSTM networks have evolved and improved [10].

Chung, J., Gulcehreet al provides a comparative analysis of different types of gated recurrent networks, including LSTMs, on various sequence modelling tasks [11].

Karpathy, A., Johnson, J., et al provide insights into how recurrent networks, including LSTMs, process sequential data. It helps in understanding the inner workings of LSTMs through visualization techniques [12]. Neha Sharma et al provide an overview of various machine learning techniques including LSTM applied to weather prediction [13].

V. METHODOLOGY

Particularly effective neural network types for sequences and time-series data, such as weather data, are RNNs and LSTMs. They can use historical data as input and infer future events based on sequence patterns. An RNN or LSTM may forecast future weather conditions in the context of weather data by using a series of historical weather variables as inputs (such as temperature, humidity, wind speed, rain, etc.). The context and the targeted prediction horizon would determine the length of the series. For instance, you might utilize a sequence of past data spanning many days as input to forecast the weather for the following day. The temporal nature of RNNs and LSTMs allows them to capture patterns and dependencies in weather data over time, making them valuable tools for tasks like weather forecasting.

VI. RECURRENT NEURAL NETWORKS (RNNs)

RNNs are made to handle data sequences by keeping a hidden state that stores knowledge about earlier time steps. The network processes each time step in a sequence along with the concealed state from the preceding time step. RNNs can now detect transient dependencies in the data. Traditional RNNs, on the other hand, may have trouble with long-term dependencies because of the vanishing gradient problem, in which the value of information from earlier time steps decreases as it spreads through the network [1]. A particular class of neural network called an RNN is made for processing data in sequences, with prior outputs serving as new inputs. As a result, RNNs may keep track of temporal connections in the data and preserve a kind of memory. The basic architecture of an RNN consists of-

Input Layer: The input sequence is supplied into the network at this point. Every component of the sequence is viewed as a separate time step.

Hidden Layer(s): The input from each time step is processed along with the previous concealed state in the hidden layer, which also keeps track of the network's internal state. However, the vanishing gradient problem, which affects vanilla RNNs, makes it difficult for them to capture long-range dependencies.

VII. LONG SHORT-TERM MEMORY (LSTM)

The vanishing gradient issue is addressed by LSTMs, a form of RNN that uses a more intricate structure with memory cells. Longer sequences of information can be selectively remembered and forgotten using LSTMs, which enables them to capture both short- and long-term dependencies. Because of this, LSTMs are very useful for time-series data, such as weather observations [1]. The architecture of an LSTM model includes-

A. *Input Layer:* Similar to RNNs, the input sequence is provided to the LSTM.

B. *LSTM Cells:* These are the heart of the LSTM architecture. Each LSTM cell contains several components:

1) *Cell State:* This represents the memory of the cell and can store information over long sequences.
2) *Hidden State:* This is the output of the cell, which carries information to the next time step and potentially to the rest of the network.
3) *Input Gate, Forget Gate, Output Gate:* These gates control the flow of information into and out of the cell.

4) *Candidate Value:* An intermediate value that could be added to the cell state.

LSTM cells are designed to allow the network to selectively remember or forget information from previous time steps, making them more capable of capturing long-range dependencies.

In terms of the number of layers, hidden units, and activation functions, these parameters can vary based on the specific problem and dataset. Generally, deeper networks and more hidden units can capture more complex patterns, but they also require more computational resources and may be prone to overfitting. Activation functions like the sigmoid or tanh functions are often used within the gates of LSTM cells to control the flow of information.

VIII. STEPS FOR WEATHER PREDICTION PROCESS USING RNNS AND LSTMS MODEL

A. *Data collection:* Historical weather data is gathered from a variety of places, including weather stations, satellites, and radar, and includes elements like temperature, humidity, pressure, wind speed, and more. The process of acquiring meteorological data entails learning about diverse atmospheric conditions at particular locations and periods. This information is essential for researching climate change, forecasting the weather, and examining weather trends. The following steps are frequently included in the data collection process:

- *Sensor Positioning:* Various sensors-equipped weather stations are carefully positioned all over the world. A variety of weather-related factors, including temperature, humidity, pressure, wind speed, wind direction, precipitation, and more, can be measured by these sensors.
- *Data Transmission:* The collected data is transmitted to central databases or servers. This can be done through wired or wireless communication channels, such as the Internet, satellite links, or cellular networks.

The Variables Collected From Weather Stations -

- *Temperature:* Both air and surface temperatures are measured.
- *Humidity:* The amount of moisture present in the air.
- *Wind Speed and Direction:* The speed and direction of the wind.
- *Precipitation:* Rainfall and other forms of precipitation.

B. *Data Preprocessing:* Preparing the data for training requires cleaning, normalizing, and otherwise preparing the acquired data. It can be necessary to manage missing values and choose characteristics depending on how well they match weather trends. Eliminate duplicates from the dataset because they can introduce bias and redundancy. eliminating them. Depending on how much information is missing, we can either discard the associated samples or use imputation methods to fill in the gaps. Mean, median, mode, or employing more complex approaches like regression imputation are examples of common imputation procedures.

C. *Model Training:* RNNs or LSTMs are constructed as neural network architectures with input layers, hidden layers containing LSTM units, and output layers for predicting specific weather variables. The model is trained on historical data, learning to capture the underlying patterns in the data.

Data Splitting Strategies: For training and evaluating RNN and LSTM models, a common strategy is to split the dataset into three main subsets: training, validation, and testing (sometimes referred to as train-validation-test split). Here's a breakdown of these subsets:

- *Training Set:* This subset is used to train the RNN or LSTM model. It typically covers the majority of the dataset and is used to learn the underlying patterns and relationships in the data.
- *Validation Set:* The validation set is used to fine-tune the model's hyperparameters and monitor its performance during training. It helps prevent overfitting and allows you to make adjustments based on how well the model generalizes to data it hasn't seen during training.

- *Testing Set:* The testing set is used to evaluate the final performance of the trained model. It provides an unbiased assessment of the model's ability to make accurate predictions on new, unseen data [12].

D. Forecasting: Once the model is trained and validated, it can be used to predict future weather conditions based on current and historical data. The model takes in a sequence of past observations and generates predictions for the next time step.

CONCLUSION

The ability to predict the weather has been much improved by the use of recurrent neural networks (RNNs) and long short-term memory (LSTM) models. In comparison to conventional approaches, these cutting-edge machine-learning techniques have shown their efficacy in understanding temporal correlations and complex patterns within weather data. The superior sequential data handling capabilities of RNNs and LSTMs make them especially well-suited for time-series data-based weather prediction applications involving observations of temperature, humidity, and pressure. They can record both short-term changes and long-term trends in weather patterns due to their capacity to store and spread information over long periods. Future improvements in hardware capabilities, model topologies, and data assimilation methods are likely to keep improving how well RNNs and LSTMs predict the weather. More accurate forecasting and more reliable predictions, particularly for extreme weather occurrences, may result from integrating these models with other data sources like satellite imaging and weather station data. Recurrent neural networks and long short-term memory models have been incorporated into weather prediction systems, which is a considerable improvement in forecast accuracy, lead time, and general comprehension of complicated weather dynamics. As technology continues to evolve, these models are poised to play a central role in advancing our ability to predict and respond to weather-related challenges.

REFERENCES

[1] X. *Shi, J. Gao, Y. Lin, & X. Yuan, "Deep learning for precipitation nowcasting: A benchmark and a new model. In Advances in neural information processing systems", AGU Journal, vol. 30, 2015, p. 561-569.*

[2] J. P. Lewis and J. M. Yellot, "A Neural Network Approach to Clustering and Forecasting Weather", 1989, p. 1-20.

[3] Y. Sun and P. Zhang, "Artificial Intelligence and Hybrid Models in the Study of Air Quality," 1997, p. 1-16.

[4] E. Kalnay, "Atmospheric Modelling, Data Assimilation and Predictability," Cambridge University vol. 2(1), 2003, p .1-18

[5] A. Weisheimer and T.N. Palmer, "Ensemble prediction using dynamically conditioned perturbations", vol. 1(1), 2005, pp. 1-9.

[6] Y. Zhang et al., "Deep convolutional neural networks for Raman spectrum recognition: A unified solution," vol. 1(1), 2015, p. 1-12.

[7] S. Hochreiter & J. Schmidhuber, "Long Short-Term Memory", Neural Computation, vol. 9(8), 1997, p 1- 32.

[8] C. Gallicchio, et al."Deep reservoir computing: A critical experimental analysis". vol. 268, 2017, p. 87-99.

[9] B. Lindemann [1], *B.* Maschler [1], *N.* Sahlab [1], *M.* Weyrich, "*A survey on anomaly detection for technical systems using LSTM networks", Elsevier, vol. 131, 2021, p. 1-9.*

[10] Greff, K., Srivastava, R. K., Koutník, J., Steunebrink, B. R., Schmidhuber, J.,"LSTM: A Search Space Odyssey". IEEE Transactions on Neural Networks and Learning Systems, vol. 1(1), 2017, p. 1-12.

[11] Chung, J., Gulches, C., Cho, K. H., & Bengio, Y., "Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling", vol. 1(1), 2014, p. 1-7.

[12] A. Karpathy, J. Johnson, & F. F. Li, "Visualizing and Understanding Recurrent Networks", vol 1(1), 2015, p.1-13.

[13] Neha Sharma, R. K. Yadav, M. S. Patterh, "A Comprehensive Survey on Weather Prediction using Machine Learning Techniques", International Journal of Computer Applications (IJCA), 2017, p.1-8.

ISSN NO : 1434-9728

Technische Sicherheit

(Technical Security Journal)

Mail : editortsjournal@gmail.com Website:https://technikwissen.eu/

Scopus And Ugc Care Group 2 Journal

Certificate of Publication

Paper Id : SJ/1419

This is to certify that the paper tittled

Decoy System-Based Approaches for Data Protection in Fog Computing: A Comprehensive Literature Review

Author by

Dr. Ujwal A. Lanjewar

From

D. B. Science College, Gondia, MS, (India).

Has been published in

TSJ, Volume 23, Issue , August 2023.

DOI:16.0006.SAH

Wilma Nchito
Editor-in-Chief

UGC APPROVED JOURNAL

Crossref

Scopus

Decoy System-Based Approaches for Data Protection in Fog Computing: A Comprehensive Literature Review

Ms. Vina L. Gautam[#1], Dr. Ujwal A. Lanjewar[#2]

[#1]*Assistant Professor, Department of Computer Science, D. B. Science College, Gondia, MS, (India)*

[#2]*Principal, Shrimati Binzani Mahila Mahavidyalaya, Nagpur, MS. (India)*

Abstract- **Fog computing has become a popular approach for enabling distributed and decentralized IoT applications, but it poses significant challenges to data protection due to various security threats. To address this challenge, decoy system-based approaches have been proposed. Decoy systems involve deploying fake resources or data to mislead attackers and divert their attention from the real resources or data. This literature review aims to provide a comprehensive overview of decoy system-based approaches for data protection in fog computing. The review highlights the key components and types of decoy systems proposed in the literature, as well as their applications and effectiveness. The insights gained from this review can help practitioners and researchers in the field of fog computing design and implement more effective data protection mechanisms. This review identifies gaps in the existing literature and suggests future research directions to enhance data protection in fog computing environments.**

***Keywords*- Fog computing, data protection, decoy, security, and privacy issues**

I. INTRODUCTION

Fog computing has emerged as a promising paradigm for enabling the deployment of Internet of Things (IoT) applications in a distributed and decentralized manner. However, one of the major challenges of fog computing is ensuring the security and privacy of data in the fog computing environment, which is vulnerable to various security threats. Decoy system-based approaches have been proposed as a potential solution to enhance data protection in fog computing. A decoy system involves deploying a set of fake resources or data to mislead attackers and divert their attention away from the real resources or data. [1] This literature review aims to provide a comprehensive overview of decoy system-based approaches for data protection in fog computing.

Fog computing represents a decentralized computing model that stretches cloud computing to the network's edge. This enables the processing and analysis of data to take place in closer proximity to where the data originates, resulting in potential reductions in latency and enhancements in response time. [2] Characteristics of fog computing include

1) *Proximity to data sources:* Fog computing is designed to process and analyze data closer to the source, which can reduce latency and improve response time.

2) *Heterogeneity:* Fog computing is designed to support a variety of devices, platforms, and operating systems, making it more flexible than traditional cloud computing.

3) *Scalability:* Fog computing is designed to scale up or down depending on the number of devices and data sources, making it more responsive to changes in demand.

4) *Security:* Fog computing is designed to be more secure than traditional cloud computing, with built-in security features such as data encryption and access controls.

5) *Resource efficiency:* Fog computing is designed to be more resource-efficient than traditional cloud computing, with the ability to process data locally and reduce the need for data transmission and storage.

A. *Challenges of data protection in fog computing environments:* Fog computing introduces new challenges for data protection due to the distributed nature of data processing and storage. Some of the challenges of data protection in fog computing environments include [3], [4], [5]

1) *Data confidentiality:* Fog computing environments involve multiple devices and networks, which can increase the risk of data breaches and unauthorized access to sensitive data.

2) *Data integrity:* Fog computing environments involve data processing and storage at the edge of the network, which can increase the risk of data corruption and manipulation.

3) *Compliance:* Fog computing environments may be subject to different regulatory requirements depending on the location of data processing and storage, which can make compliance challenging.

4) *Interoperability:* Fog computing environments involve multiple devices and platforms, which can make it challenging to ensure interoperability and compatibility of data protection mechanisms.

5) *Resource constraints:* Fog computing environments may have limited resources, such as processing power and storage capacity, which can make it challenging to implement robust data protection mechanisms.

B. *Decoy systems and their key components:* Decoy systems, also known as honeypots, are computer security mechanisms that are designed to detect, deflect, or study unauthorized access to information systems. They work by mimicking vulnerable systems or services, which can attract attackers and divert their attention away from critical systems. [6], [7], [8] The key components of decoy systems include:

1) *Bait:* The bait is the component of a decoy system that is designed to attract attackers. This can include software, hardware, or data that appears to be valuable or vulnerable to attack.

2) *Monitoring and logging:* Decoy systems must be able to monitor and log all activity to detect and analyze attacks. This includes network traffic, system logs, and other data that can provide insight into attacker behavior.

3) *Alerting and response:* When an attack is detected, a decoy system must be able to alert security personnel and initiate a response. This can include shutting down the decoy system, blocking the attacker's IP address, or collecting additional information about the attack.

4) *Isolation:* Decoy systems must be isolated from critical systems to prevent attackers from gaining access to sensitive data or resources. This can include virtualization, network segmentation, or physical separation.

II. REVIEW OF LITERATURE

The findings of this literature review will contribute to the understanding of the effectiveness and limitations of decoy system-based approaches for data protection in fog computing. It will also identify gaps in the existing literature and suggest future research directions. The insights gained from this review can help practitioners and researchers in the field of fog computing to design and implement more effective data protection mechanisms.

Following decoy-based approaches can be used individually or in combination to protect data in fog computing

A) *Honeypot-based decoy system:* A honeypot-based decoy system can effectively protect data in fog computing by luring attackers away from sensitive data. The paper proposes a honeypot-based secure network system that aims to detect and prevent network attacks by deploying honeypots.

The authors discuss the design and implementation of the system, which includes the deployment of multiple honeypots that mimic various types of servers and services to attract potential attackers. [9]

B) *Deceptive routing-based decoy system:* Deception is used to distract attackers from attacking legitimate routes for real data. A deceptive routing-based decoy system can help to confuse attackers by leading them down fake paths.[10]

C) *AI/ML-based security approach:* The paper titled "SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications" by [11] proposes a secure offloading system for smart city applications using a combination of fog and cloud computing. The authors address the security concerns associated with offloading by proposing a machine learning-based approach that can identify malicious activities. The paper describes the design and implementation of the SecOFF-FCIoT system, which includes a security module that uses machine learning algorithms to detect and prevent attacks. [11]

D) *Blockchain-based security approach:* A blockchain-based security approach can help to ensure the integrity and confidentiality of data in fog computing. [12] proposed a blockchain-based approach for secure data sharing in fog computing, which was found to be effective in protecting sensitive data.[12]

E) *Attribute-based encryption-based security approach:* An attribute-based encryption (ABE)-based security approach can be used to protect sensitive data in fog computing by allowing access only to authorized users with specific attributes. A study by [13] analyzed the performance of ciphertext-policy attributed-based encryption (CP-ABE) algorithms in fog computing and found them to be effective in providing fine-grained access control.[13]

F) *Hardware-based security approach:* A hardware-based security approach can be used to protect fog computing systems by providing secure storage and processing capabilities. The authentication scheme based on PUFs works by using the unique responses generated by each device's PUF as a basis for authentication. When a device needs to be authenticated, it sends its PUF response to a central server. The server then verifies the response against the device's pre-registered PUF response, which acts as a unique identifier for the device. If the two responses match, the device is authenticated and granted access to the requested information or services. Overall, this PUF-based authentication scheme is an effective way to protect the security and privacy of confidential information stored on edge devices, while also being resource-efficient and requiring minimal hardware. [14]

G) *Software-defined networking-based security approach:* The framework based on Software-Defined Networking (SDN) provides scalability, flexibility, programming capability, and global information, while Fog computing offers sophisticated and location-aware services that can fulfill the future requirements of Vehicular Ad Hoc Networks (VANETs). [15] proposed an SDN-based security framework for fog computing, which was found to be effective in providing security. [15]

H) *Intrusion detection-based security approach:* An intrusion detection-based security approach can be used to protect fog computing systems by detecting and responding to attacks in real-time. The article proposed by [16] presents an extensive examination and evaluation of the architecture of Fog Computing, along with the potential security challenges and attacks associated with it. Furthermore, it explores the usage of intrusion detection systems to minimize the impact of these problems in a Fog environment. The article thoroughly analyzes the previous works in this domain and comprehensively outlines their challenges and limitations.[16]

I) *Continuous monitoring-based security approach:* A continuous monitoring-based security approach can be used to protect fog computing systems by continuously monitoring for security threats and

responding in real time. [17] proposed a continuous monitoring system for cloud computing, which was found to be effective in detecting and responding to security threats in real-time. [17]

J) *Behavioral-based security approach:* To safeguard fog computing systems, a security approach based on behavior analysis can be implemented. This approach involves scrutinizing the actions and conduct of users and devices to identify any irregularities or potential security risks. As specified in the paper by [18]. By monitoring behavioral patterns, anomalies can be detected and potential threats can be identified, leading to enhanced protection for fog computing systems. [18]

K) *Access control-based security approach:* Implementing access control mechanisms helps regulate and restrict data access based on user roles, privileges, and authentication. This ensures that only authorized individuals or devices can access and manipulate sensitive data. This article published by [19] presents a thorough examination of user data access control in the context of fog computing, focusing on identifying security issues and challenges. It covers the definition, structure, and features of fog computing, and subsequently explores the typical access control requirements and fundamental models associated with it.[19]

L) *Security approach based on Ciphertext-policy attribute encryption:* Fan and colleagues highlight the potential of Ciphertext-policy attribute-based encryption (ABE) in enabling data access control in fog-cloud systems. To address this, they present an access control scheme that relies on a verifiable outsourced multi-authority model. [20]

M) *Security approach based on blind quantum computation:* [21] proposed a quantum fog computing model based on blind quantum computation and verifiable quantum secret sharing. The primary reliance of the proposed model lies in blind quantum computation to achieve the desired security features encompassing multiple fog nodes. By utilizing the quantum secret sharing protocol, the model offers characteristics such as identity verification and channel detection protection. This approach efficiently fulfills the functionalities of conventional fog computing while simultaneously ensuring the secure transmission of information and data computations. [21]

N) *Key management-based security approach:* A key management-based security approach can be used to protect fog computing systems by securely managing cryptographic keys used for encryption and decryption. In the article written by [22], a key management system utilizing hypergraph schemes is proposed to address security needs and account for the unique characteristics of the environment. The fog computing architecture, with its three-tier hierarchy, is divided into two subnetworks based on the key hypergraph. Additionally, specific key management processes are devised for each subnetwork to meet the operational and security requirements of fog computing. The performance evaluation and numerical simulation demonstrate that the proposed scheme exhibits low key generation costs and overhead. This implies that the scheme can be utilized effectively to construct an efficient and secure system for fog computing. [22]

Overall, these approaches demonstrate the importance of implementing effective security measures in fog computing systems to protect against a range of security threats. However, it is important to note that no single approach can provide complete security for fog computing systems, and a combination of approaches may be necessary to provide comprehensive protection.

III. STRENGTHS AND LIMITATIONS

Decoy system-based approaches for data protection in fog computing have several strengths and limitations.

A) *Strengths:*

1) *Effective in detecting and preventing attacks:* Decoy systems can be used to detect and prevent attacks by diverting attackers from the actual system and providing a false target for them to attack.

This can help protect the actual system and data from security threats.

2) *Cost-effective:* Decoy systems are generally less expensive than actual systems and can be used to provide an additional layer of security without significant additional costs.
3) *Easy to deploy:* Decoy systems are easy to deploy and can be set up quickly to provide an additional layer of security.
4) *Provides early warning:* Decoy systems can provide early warning of potential security threats by detecting and diverting attackers before they can cause any damage to the actual system.

B) *Limitations:*

1) *May not provide complete protection:* Decoy systems may not provide complete protection against all types of attacks, and attackers may eventually discover the real system and data.
2) *May increase complexity:* The use of decoy systems may increase the complexity of the overall system, which may make it harder to manage and maintain.
3) *May increase false positives:* Decoy systems may generate false positives, which can be time-consuming and costly to investigate and resolve.
4) *May be limited in effectiveness:* Decoy systems may be limited in effectiveness against sophisticated attackers who can bypass or ignore them.
5) *May require additional resources:* Decoy systems may require additional resources such as storage, processing power, and bandwidth, which can increase costs and complexity.

In summary, decoy system-based approaches can be an effective tool for protecting data in fog computing systems, but they may have limitations in terms of complete protection increased complexity, and false positives. It is important to consider these factors when choosing and implementing decoy system-based approaches for data protection in fog computing.

IV. RESEARCH GAP

Although decoy system-based approaches have shown promise for data protection in fog computing, there are still several gaps and areas for future research that need to be addressed. Some potential research directions include:

1) *Development of more effective decoy systems:* Future research could focus on developing more advanced and sophisticated decoy systems that are capable of detecting and deterring a wider range of attacks.
2) *Integration with other security measures:* Decoy systems can be used in conjunction with other security measures such as encryption, access control, and intrusion detection systems to provide comprehensive protection for fog computing systems. Research could focus on developing methods to integrate these security measures with decoy systems to provide more effective protection.
3) *Evaluation of effectiveness:* There is a need to conduct more extensive empirical evaluations of the effectiveness of decoy system-based approaches for data protection in fog computing. This would involve testing the approaches in a variety of scenarios and under different types of attacks.
4) *Scalability:* Decoy system-based approaches need to be scalable to support large-scale fog computing environments with a large number of devices and users. Research could focus on developing scalable decoy systems that can provide effective protection in such environments.
5) *Optimization of resource utilization:* Decoy systems may require additional resources such as storage, processing power, and bandwidth, which can increase costs and complexity. Future research could

focus on developing methods to optimize resource utilization in decoy system-based approaches to reduce costs and complexity.

6) *Privacy protection:* Decoy systems can collect data on attackers and their behavior, which raises privacy concerns. Future research could focus on developing methods to protect the privacy of users while still maintaining the effectiveness of decoy systems.

Overall, future research should focus on developing more advanced and effective decoy system-based approaches for data protection in fog computing, while also addressing the challenges and limitations of these approaches.

CONCLUSION

In conclusion, data protection is a critical issue in fog computing due to the distributed nature of the environment and the potential for various security threats. Decoy system-based approaches have emerged as a promising method for protecting fog computing systems and data from security threats. These approaches involve deploying decoy systems that are designed to detect and divert attackers away from the actual system and data, providing an additional layer of security.

This review identified various decoy system-based approaches for data protection in fog computing and provided a summary of their strengths and limitations. The approaches included a range of techniques such as honeypots, blockchain, machine learning, and behavior monitoring, among others. While these approaches have shown promise, further research is still needed to optimize and enhance their effectiveness in detecting and deterring security threats.

Overall, decoy system-based approaches are important for protecting data in fog computing systems. However, they are not a complete solution and should be used in conjunction with other security measures to provide comprehensive protection. Future research should focus on developing more advanced and effective decoy system-based approaches, evaluating their effectiveness, and addressing the challenges and limitations of these approaches to enhance data protection in fog computing.

REFERENCES

[1] S. Khan, S. Parkinson, Y. Qin. “Fog computing security: a review of current applications and security solutions”, Journal of Cloud Computing. Dec. 2017, vol. 6, pp.1-22.

[2] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, JP. Jue JP. “All one needs to know about fog computing and related edge computing paradigms: A complete survey”, Journal of Systems Architecture. Sep. 2019; vol.98, p. 289-330.

[3] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, MA. Ferrag, N. Choudhury, V. Kumar. “Security and privacy in fog computing: Challenges”, IEEE Access. Sep. 2017, vol. 5.

[4] MR. Raza, A. Varol, N. Varol. “Cloud and fog computing: A survey to the concept and challenges. In 2020”, 8th International Symposium on Digital Forensics and Security (ISDFS), Jun. 2020, p. 1-6, IEEE.

[5] P. Zhang, M. Zhou, G. Fortino. “Security and trust issues in fog computing: A survey”, Future Generation Computer Systems. Nov. 2018.

[6] BM. Bowen, S. Hershkop, AD. Keromytis, SJ. Stolfo. “Baiting inside attackers using decoy documents. In Security and Privacy in Communication Networks”, 5th International ICST Conference, SecureComm, Athens, Greece, Sept. 2006, p. 14-18.

[7] S. Pothumani, C. Anuradha. “Decoy method on various environments - A survey. International Journal of Pure and Applied Mathematics”, 2017, vol. 116(10), p. 197-200.

[8] KP. Bindu Madavi, P. Vijayakarthick. “Decoy technique for preserving the privacy in fog computing. In Evolutionary Computing and Mobile Sustainable Networks”, Proceedings of ICECMSN, Springer Singapore 2020, p. 89-94.

[9] YK Jain, S. Singh. “Honeypot based secure network system. International Journal on Computer Science and Engineering’, Feb. 2011, vol. 3(2), p. 612-20.

[10] Zhu, Quanyan & Clark, Andrew & Poovendran, Radha & Başar, Tamer. “Deceptive routing games”, Proceedings of the IEEE Conference on Decision and Control, 2012, pp. 2704-2711. 10.1109/CDC.2012.6426515.

[11] AA. Alli, MM Alam. “SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications. Internet of Things”, Sep. 2019.

[12] O. Umoren, R. Singh, S. Awan, Z. Pervez, K. Dahal. “Blockchain-Based Secure Authentication with Improved Performance for Fog Computing. Sensors”, Nov. 2022.

[13] M. Alshehri, B. Panda. “An encryption-based approach to protect fog federations from rogue nodes. InSecurity, Privacy, and Anonymity in Computation, Communication, and Storage”, 12th International Conference, SpaCCS, Atlanta, GA, USA, Springer, July 2019. p. 225-243.

[14] CH. Chang, Y. Zheng, L. Zhang. “A retrospective and a look forward: Fifteen years of physical unclonable function advancement”, IEEE Circuits and Systems Magazine, Aug. 2017, vol. 17, p. 32-62.

[15] M. Arif, G. Wang, T. Wang, T. Peng. “SDN-based secure VANETs communication with fog computing. InSecurity, Privacy, and Anonymity in Computation, Communication, and Storage: 11th International Conference and Satellite Workshops, SpaCCS 2018, Melbourne, NSW, Australia, Dec. 2018, p. 46-59. Springer International Publishing.

[16] FA. Zwayed, M. Anbar, Y. Sanjalawe, S. Manickam. “Intrusion Detection Systems in Fog Computing–A Review. InAdvances in Cyber Security”, Third International Conference, ACeS 2021, Penang, Malaysia, Aug. 2021, p. 481-504.

[17] AK. Yadav, ML. Ritika, ML. Garg. “Monitoring Based Security Approach for Cloud Computing. Ingénierie des Systèmes d Inf”, Dec. 2019, vol. 24(6).

[18] SJ. StolfoJ, MB Salem, AD Keromytis. “Fog computing: Mitigating insider data theft attacks in the cloud”, In IEEE symposium on security and privacy workshops May 2012, p. 125-128. IEEE.

[19] P. Zhang, JK. Liu, FR. Yu, M. Sookhak, MH Au, X. Luo. “A survey on access control in fog computing’, IEEE Communications Magazine, Feb. 2018, vol. 56(2).

[20] K. Fan, J. Wang, X. Wang, H. Li, Y. Yang. “A secure and verifiable outsourced access control scheme in fog-cloud computing. Sensors”, Jul. 2017, vol. 17(7).

[21] Z. Qu, K. Wang, M. Zheng. “Secure quantum fog computing model based on blind quantum computation”, Journal of Ambient Intelligence and Humanized Computing, Aug. 2021.

[22] Z. Li, Y. Liu, D. Liu, C. Li, W. Cui, G. Hu. “A key management scheme based on hypergraph for fog computing”, China Communications. Nov. 2018, vol. 15(11).