IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

# Prevention of Key Recovery Attacks Using Optimized Anomaly Based Intrusion Detection Mechanism

**Alias Itten[1], Soumya K S[2]**

Lecturer, Dept. of Computer Engineering, Govt. Polytechnic College, Kaduthuruthy, India[1]

Lecturer, Dept. of Computer Engineering, Govt. Polytechnic College, Cherthala, India[2]

**ABSTRACT:** With the growing popularity in wireless network technologies and services, privacy has become a top priority. Data security as well as authenticity is key security concerns for information management. As a result, computer network security as well as availability is becoming top concerns, making it a critical tool to maintain. To ensure communication security in systems, a preventative technique is required. Because the network is vulnerable to assaults like grey-hole (GH) attacks, wormhole (WH) attacks, and black-hole (BH) attacks, the sender nodes are unable to deliver messages to the target node owing to malevolent activity. To protect the network from attacks this study introduces a strategy called African Buffalo based keyed intrusion detection system (ABKIDS). This method is used to protect the network from wormhole attacks and other harmful activity. So, based on the survey, a scheme is to be conducted that will enable us to offer greater protection on cloud data storage and on personal computers. Thus, the suggested method will provide extra safety that would be utilized for securing sensitive data from multiple domains, such as patient related information like contact information and history in the healthcare industry.

## I. INTRODUCTION

The use of the internet is rising dramatically in modern years. The majority of people utilised the network to transfer data and the cloud to store it (Mishra, et al. 2018). As a result, there is a chance that the data will be accessed and misused. Several anomaly intrusion detection systems have been established in recent years to provide greater security (Juan E. Tapiador, et al. 2015) from certain unwanted users. The safety issue (M. Barreno et al. 2010) is primarily classified into two categories: malicious attack and non-harmful attacks. The harmful attack is an attack to violently misuse or exploit other's computer, (R. Sommer, et al. 2010) either by social engineering, computer viruses, phishing, or even other forms of social engineering. Most computer network security issues can be overcome (B. Biggio, et al. 2011) by distinguishing between harmful and non-malicious attacks (K. Wang, et al. 2006). In fact, determining what is safe and what is harmful is a difficult task. To solve these challenges, the majority of these challenges used a typical machine-learning technique (K. Rieck, 2011), in which classifiers are being utilized to spontaneously build structures of (bad or good) behavior, which are then utilized in identifying possible risky events.

An Intrusion Detection System (IDS) is a utility and program package which observers the architecture of a system which performs malicious behaviors or intrusion breaches and sends reports to a command centre (Gupta, Prasad, and Nayak 2019). The two main types of anomaly-based IDS are: Network based Intrusion Detection Systems (NIDS) as well as Host based Intrusion Detection Systems (HIDS). NIDS is a network based IDS which examines network connections for numerous devices or servers (Sarkar, et al. 2016). HIDS keeps track of a particular host or client. Several assaults including (DoS) Denial of Service, Black Hole, Distributed DoS (DDoS), Grey Hole attacks, as well as Worm Hole attacks, are attacking the network. Furthermore, the problems of misbehaving routing are among the widely diffused network terrorizations, similar to BH attacks (Rana et al. 2015). As a result, various researchers have proposed a variety of secured routing approaches to address these challenges, but network security remains a concern (Jamal, et al. 2019). Thus, different protection methods have been implemented to prevent malicious attacks, although they have encountered numerous difficulties (Ananthakumaran, et al. 2020).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

To ensure safe communication, various routing protocols such as artificial intelligence (Ghathwan, Khalil, et al. 2014), EMAODV, and the Ad-hoc On-demand Distance Vector (AODV) method is presented (D Toradmalle, et al. 2019). Malicious actions, on the other hand, generate trustworthy nodes, to which the sender sends information (Panigrahi, et al. 2015). However, it will not be able to reach the intended receiver since the attacker sends data to the third party. Hence, the suggested method uses an African buffalo optimization for anomaly based intrusion detection as discussed in this research. The proposed approach boosts network performance while also ensuring network security. The following are the sections of this work: Section 2 discusses relevant studies and the current state of art in the area of Intrusion Detection Systems. Section 3 presents the expert system that was used to identify network anomalies. The representative obtained outcomes are discussed in Section 4. Lastly, Section 5 summarizes the findings of this paper.

## II. RELATED WORKS

In this segment, we survey the existing literature on IDS frameworks.

According to M. E. L. Ajjouri et al. (2016), the improvement of data structures necessitates the use of an unstable state of protection in order to limit the problems that these structures may cause. Intrusion Detection Systems (IDS) play a key role in protection measures by detecting when an attack is underway; yet, most existing Intrusion Detection System have been grouped together and are suffering the consequences of notable restrictions. In view of adopting new threats, this study illustrates another security analyst engineering. . We demonstrate the approach's idea and portrayal; at that time, the method used for training is Case based Reasoning (CBR). We also use the AUML dialect to present our assessment program. However, the design is not put into action to check the different structures and to confirm that the goal is met.

The authors of this research (Divyatmika and M. Sreekesh, 2016) have presented a method for detecting and uncovering fresh threats. Because a page could be used by a large number of people, maintaining the resources accessible and assigning them to variable clients based on their needs is critical. The multithread concept is used for sharing resources that are available to all customers. In Weka, the Quality Selection Method is utilized as the component removal method to produce these significant aspects related to client's requirement as well as aids to achieve more accurate outcome. The falling paired inquiry tree provides memory efficiency. The instances are properly saved, and thus the search for the presence of an assault is sufficiently refined. This method proposes an Intrusion Detection System that is memory proficient and sufficiently competent in identifying assaults while reducing false positives.

In this method (T. Zou et al. 2016), Intrusion Detection Systems plays a key role in the network safety. The basic test is the method for locating instances of examples defined in the given set that depict the mark of malware attacks. In light of the bit parallel technique, the authors provided a productive proper description organizing algorithm in this study. Our method outperforms the traditional Aho-Corasick machine with less false positives, according to preliminary results. They developed an Intrusion Detection System separation algorithm that was somewhat parallel. It is quicker than the standard Aho-Corasick automata. Regardless of the fact that it produces a small number of false positive responses, it could be accepted as it perform the usual articulation coordination a little time afterwards.

According to this study, (Sharafaldin, et al. 2018) since 1998 over eleven public datasets, many dataset is being out of service and undependable for using. Certain datasets do not cover various attacks, and certain datasets lose volume and traffic diversity, where others anonymized data packets as well as payloads that could not replicate present trends and missing metadata and feature sets. This study creates a trustworthy dataset with seven similar network attack flows that fit actual requirements that are available in public. The study compares the performance in a wide range of network machine learning methods as well as traffic metrics to determine which characteristics are effective for detecting specific attack types. However, the number of PCs must be increased in the future, and also more up-to-date attacks must be carried out.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

In this research (I. Lee et al. 2012), the authors present a novel string looking technique and an Intrusion Detection System based on it. Furthermore, as part of our background research, they looked into a few accurate example searching methods and their identical inspection. The suggested IDS is evaluated using a five-thousand-record dataset (a subset of the KDD Cup dataset) with forty-one highlights. It is possible to complete the IDS by evaluating global nucleotide configurations of a large number of dataset highlights. They also provided a creative string coordinating algorithm in their research, which aided in forming IDS. As a result, they used a DNA encoding method in which all of the features of every record are turned into nucleotide sequence.

## III. PROPOSED METHOD

Attacks are quite effective, indicating that recovering the key is relatively simple for an attacker. As a result, a lack of safety exposes that approaches like African buffalo are meant to protect key-recovery assaults in the first place. The suggested technique, on the other hand, ensures secure communication from sender to receiver in networks. In the beginning, a communication channel is created in the network that is weak to several attacks like Black hole attack, Wormhole attack, and Grey hole attack. As a result, this technique employs an original African buffalo based keyed intrusion detection system to protect communication channels against hostile activity. Finally, this technique serves as a network-wide defense mechanism against destructive attacks. The suggested solution aims to protect the network from harmful behaviour before it happens. The proposed approach and the operation of African buffalo based keyed intrusion detection system in malicious activity are depicted in Fig. 1.

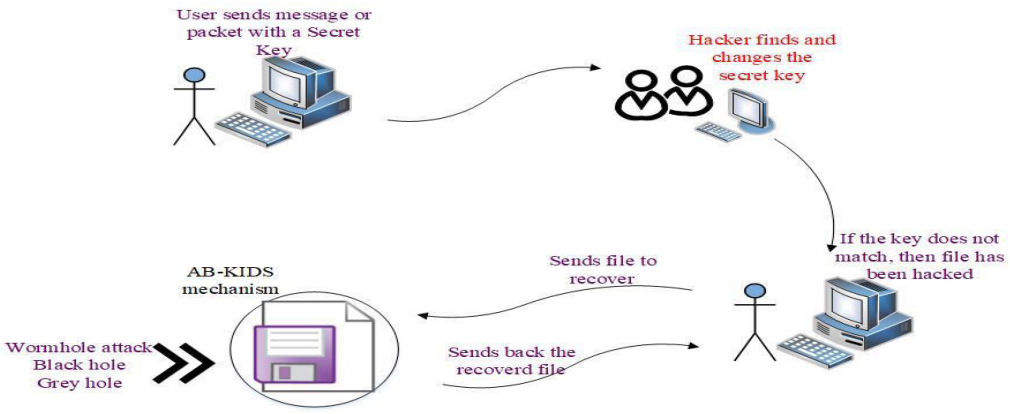


Fig. 1 Proposed AB-KIDS mechanism

*3.1 African Buffalo based keyed intrusion detection system*

African Buffalo based keyed intrusion detection system (AB-KIDS) is a hybrid version of the African buffalo. In this method, hostile nodes are anticipated utilizing AB-KIDS's optimization technique, and a new encrypted communication path is identified. Firstly, the AB-KIDS protocol establishes a data transfer routing zone. This routing zone contains a large number of nodes (N), all of which are connected to the communication system. Originally, the source hub sends data packets to the recipient via surrounding nodes, forming a packet transmission channel. The suggested solution recognizes the affected nodes and produces good transmission through an alternative method because network is weak to malicious activity. The suggested AB-KIDS model recognizes attacks like the Worm hole, Black hole, and Grey hole attacks. This method starts with the network zone (N).

**Algorithm 1: AB-KIDS for attack prevention**

Start

{

Set up network communication (N)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

Create sender (S) and receiver (R);
Using eqn.(1) determine the energy levels of all the networks
If $E_T(N) > 1J$ // harmful activity is present
then
Determine the energy threshold for all the networks
$1J < E_T(w) > 1.5\ J$ // $E_T(w)$ represents the energy threshold of wormhole attack
$1.5\ J < E_T(b) > 2\ J$ // $E_T(b)$ represents the energy threshold of black hole attack
$2\ J < E_T(g) > 2.5\ J$ // $E_T(g)$ represents the energy threshold of grey-hole attack
end
notify the source node; // S node does not transfers the message in this path
Select the optimal path // safe communication
end-if
}
Stop

Subsequently, after detecting the malicious nodes, AB-KIDS detects attacks such as Worm Hole, Black Hole, and Grey Hole depending on the energy levels of harmful nodes. Therefore, the node's energy threshold is determined using eq. (1).

$$E_T(N) = \frac{EReq + ERply}{\mu} \quad (1)$$

Where, $E_{Req}$ is signifies the energy for Req message, $E_{Rply}$ is represents the energy for Rply message and μ denotes the energy of the attacks.

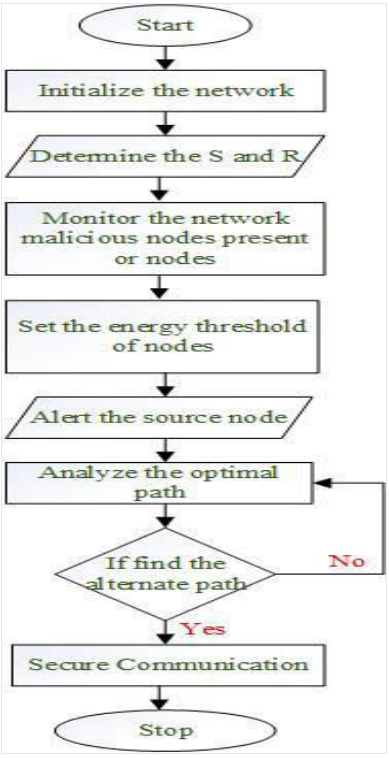


Fig. 2 Flowchart of proposed method

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

In this method, the ABKIDS continuously analyses the network for malicious nodes. If it detects potentially dangerous nodes, it notifies the source node and enables secure communication via the best channel, as shown in Fig. 2.

## IV. RESULTS AND DISCUSSION

Our attacks have been experimentally verified in python. 2000 HTTP packets recorded in a university network were used to train the system. Each node will be authenticated by the ABKIDS mechanism. Every user would submit their files including a secret key that was created just for them. Users who do not have access to the Secret key will be unable to upload files. AB-KIDS mechanism will also deliver an alert message about the attacker after wormhole, grey hole and black hole attacks, and would continue with preventative procedures based on the training data. The suggested model's accuracy and efficacy are assessed using existing methods.

### *4.1 Performance metrics*

Precision, recall, accuracy, as well as F-measure are some of the performance indicators utilized in assessing the effectiveness of the suggested method. The main factors are, Tn', Fn', Tp' as well as Fp', which stands for true negative, false negative, true positive, and false positive.

#### 4.1.1 Precision:

The percentage ratio of the number of true positives (Tp') records divided by the sum of true positives (Tp') and false positives (Fp') classified records is known to be precision (P).

$$\text{Precision} = \frac{Tp'}{Tp'+Fp'} \times 100 \tag{2}$$

#### 4.1.2 Recall:

The percentage ratio of the number of true positives records divided by the total of true positives and false negatives (Fn') classified records is known as recall (R).

$$\text{Recall} = \frac{Tp'}{Tp'+Fn'} \times 100 \tag{3}$$

#### 4.1.3 F-Measure (F):

The harmonic mean of recall and precision is expressed as the F-measure, which indicates a balance between the two.

$$\text{F-measure} = 2\left(\frac{P \times R}{P + R}\right) \tag{4}$$

The following Fig. 3 depicts the performance comparison of the proposed technique with the existing Self-taught Learning (STL), a deep learning based method (Javaid et al. 2016) with F-measure, recall and precision.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

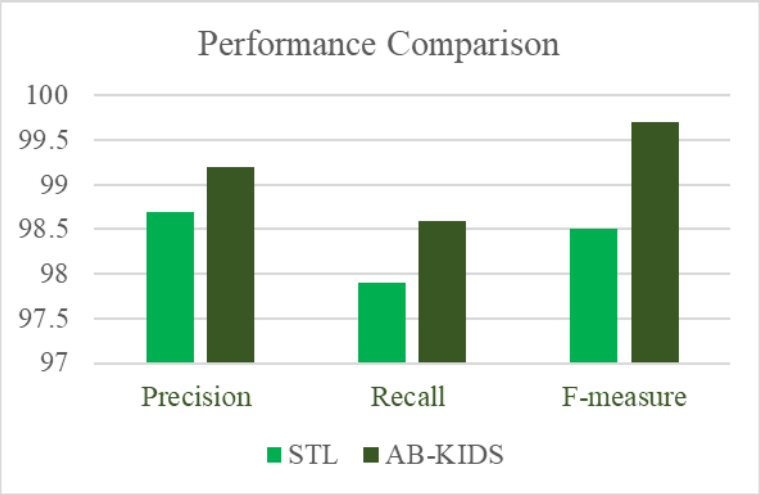


Fig. 3 Performance comparison

| | Upload Time | Hack Time | Recovery |
|---|---|---|---|
| File 1 | 190 | 540 | 198 |
| File 2 | 160 | 330 | 172 |
| File 3 | 750 | 450 | 160 |
| File 4 | 245 | 590 | 160 |

Table 1 System performance

Table 1 displays the time calculation of hacking time and recovery time. The Plotted graph based on time calculation explains how the AB-KIDS mechanism is recovering the key in less time than the hacking time is shown in Fig. 4.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

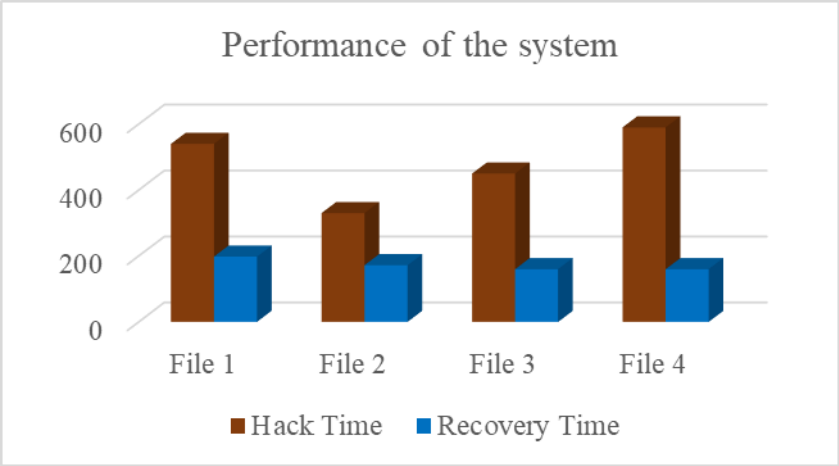


Fig. 4 Performance graph of the system

## V. CONCLUSION

The rising warning of intrusion detection is causing havoc for networking groups as well as other organisations. This paper has discussed and reviewed some of the most effective tactics offered by many scientists in this subject. This investigation has definitely aided me in proposing in my personal study effort and producing something exceptional. The loss of information based on the classifier which tries in inhibiting evasion by depending on a hidden piece of data will be limited if we use this methodology. The effectiveness of the suggested Intrusion Detection System in this study is superior to that of other present machine learning techniques, and it can detect practically all anomalous data in the computer system. The suggested work could be used in the future to compute different distance computation functions between both the trained model and the testing data. Our research could be used to increase the accuracy of IDS in a more effective way.

## REFERENCES

1. Sarkar, J.L., Panigrahi, C.R., Pati, B., Das, H.: A novel approach for real-time data management in wireless sensor networks. In: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, pp. 599–607. Springer, New Delhi (2016).
2. Mishra, B.B., Dehuri, S., Panigrahi, B.K., Nayak, A.K., Mishra, B.S.P., Das, H.: Computational intelligence in sensor networks. In: Studies in Computational Intelligence, vol. 776. Springer (2018).
3. Panigrahi, C.R., Sarkar, J.L., Pati, B., Das, H.: S2S: a novel approach for source to sink node communication in wireless sensor networks. In: International Conference on Mining Intelligence and Knowledge Exploration, pp. 406–414. Springer, Cham, Dec 2015.
4. Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos, “Key-Recovery Attacks on KIDS, a Keyed Anomaly Detection System”, IEEE Transactions on Dependable and Secure Computing, Vol. 12, No. 3, May/June 2015.
5. M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar, “The Security of Machine Learning,” Machine Learning, vol. 81, no. 2, pp. 121-148, 2010.
6. B. Biggio, B. Nelson, P. Laskov. “Support Vector Machines under Adversarial Label Noise.” In Journal of Machine Learning Research - Proceedings Track, Vol. 20, pp. 97–112, 2011.
7. K. Wang, J. Parekh, and S. Stolfo, “Anagram: A Content Anomaly Detector Resistant to Mimicry Attack,” Proc. Ninth Int’l Conf. Recent Advances in Intrusion Detection (RAID ’06), pp. 226-248, 2006.
8. K. Rieck, “Computer Security and Machine Learning: Worst Enemies or Best Friends?” Proc. DIMVA Workshop Systems Security (SYSSEC), 2011.
9. R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” Proc. IEEE Symp. Security and Privacy, pp. 305-316, 2010.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912039 |

10. Ghathwan, Khalil I., and Abdul Razak B. Yaakub. "An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET." Recent Advances on Soft Computing and Data Mining. Springer, Cham, 2014. 121-131.
11. Rana, Anuj, VinayRana, and Sandeep Gupta. "EMAODV: Technique to prevent collaborative attacks in MANETs." Procedia Computer Science 70 (2015): 137-145.
12. D Toradmalle, J Muthukuru, B Sathyanarayana," Certificateless and provably-secure digital signature scheme based on elliptic curve."- International Journal of Electrical & Computer Engineering (2088-8708)- 2019.
13. Jamal, Tauseef, and Shariq Aziz Butt. "Malicious node analysis in MANETS." International Journal of Information Technology 11.4 (2019): 859-867.
14. Ananthakumaran.S, Debrup Banerjee, P. G. Om Prakash, R. Bhavani, "Fuzzified Energy Efficient Mechanism (FEEM) in Wireless Sensor Network," International Journal of Emerging Trends in Engineering Research, Vol. 8, No. 9, pp. 6889-6396, September, 2020.
15. M. E. L. Ajjouri, "New Model of Intrusion Detection Based On Multi Agent Systems andCBR Paradigm," pp. 133–138, 2016.
16. Divyatmika and M. Sreekesh, "A two-tier network based intrusion detection system architecture using machine learning approach," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016 IEEE, pp. 42-47
17. T. Zou, Y. Cui, M. Huang, and C. Zhang, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.
18. Sung-Il Oh, Inbok Lee and Min Sik Kim, "Fast filtering for intrusion detection systems with the shift-or algorithm," 2012 18th Asia-Pacific Conference on Communications (APCC), Jeju Island, 2012 IEEE, pp. 869-870
19. El Ajjouri, Mohssine, Siham Benhadou, and Hicham Medromi. 2016. "New Model of Intrusion Detection Based on Multi Agent Systems and CBR Paradigm." In *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, 133–38. Tangier, Morocco: IEEE. https://doi.org/10.1109/CIST.2016.7805030.
20. Gupta, Amara S. A. L. G. Gopal, G. Syam Prasad, and Soumya Ranjan Nayak. 2019. "A New and Secure Intrusion Detecting System for Detection of Anomalies Within the Big Data." In *Cloud Computing for Geospatial Big Data Analytics*, edited by Himansu Das, Rabindra K. Barik, Harishchandra Dubey, and Diptendu Sinha Roy, 49:177–90. Studies in Big Data. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-03359-0_8.
21. Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. 2016. "A Deep Learning Approach for Network Intrusion Detection System." In *Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS)*. New York City, United States: ACM. https://doi.org/10.4108/eai.3-12-2015.2262516.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com



Scan to save the contact details