International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

A Data-Driven Network Security Situation Awareness Model Using Locality Sensitive Hashing

G. Preethi[1], B. Pravalika[2]
[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana – 501301, India.
[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana – 501301, India.

***Abstract* – Network information transmission security has become more complicated due to the ever-increasing complexity of digital communication infrastructures and the ever-increasing volume of network traffic. When dealing with large-scale data settings, traditional methods of network security monitoring may be inefficient and hard to adjust to. In light of these difficulties, this research proposes an LSH-based data-driven paradigm for situational awareness in network security. The suggested architecture analyses and monitors network events in real-time to spot suspicious patterns that might represent security risks. In order to effectively find similar patterns and detect anomalous occurrences, the LSH algorithm is used after data preparation and feature analysis to the network information. To further assess its efficacy in security scenario awareness, the suggested method is compared to the Bayesian algorithm. The LSH algorithm outperforms the Bayesian method, which yields a detection rate of 80% to 85%, according to experimental study, which falls anywhere between 90% and 95%. Furthermore, the LSH-based method consistently identifies anomalies in networks with a fidelity and accuracy that surpasses that of traditional methods, with a false detection rate that remains below 1%. By maintaining the original methodology and experimental evaluation, the proposed framework efficiently improves the security of network information transmission by helping to identify threats faster, increasing situational awareness, and making large-scale communication environments more resilient.**

***Keywords* – Network Security, Situation Awareness, Locality Sensitive Hashing, Data Analysis, Network Information Transmission, Anomaly Detection, Bayesian Algorithm, Cybersecurity, Data Mining.**

I. INTRODUCTION

The generation, transmission, and access of information via contemporary computer networks have been revolutionised by the fast development of digital communication technology. There has been a dramatic surge in network traffic due to the proliferation of internet services, cloud computing, industrial systems, financial transactions, and essential public services that rely on large-scale network infrastructures. While these advancements have made communication more efficient and accessible, they have also brought forth major security concerns. The availability, integrity, and confidentiality of network information are still under risk from cyberattacks, illegal access, harmful malware, and suspicious network activity. As a result, providing safe transmission of data via networks is now a top priority for cybersecurity researchers.

In order to detect suspicious actions, traditional network security measures often use signature databases, predetermined rules, and human analysis. While these methods still perform well against common types of assaults, they aren't always up to the task of detecting complex new threats across networks with thousands of nodes. Traditional approaches to security management have also become less successful due to the computational overhead of real-time monitoring brought on by the exponential expansion of network data. Because of these restrictions, scientists are looking at smart data analysis methods that may detect unusual network activity automatically without sacrificing processing performance.

An essential method for comprehending the general state of communication environment security, Network Security Situation Awareness (NSSA) involves constantly watching network activity, evaluating security occurrences, and forecasting any dangers. By combining data from many security sources, situation awareness gives a holistic view of the network's state, as opposed to only concentrating on specific assaults. Network administrators may prevent security issues from becoming worse by constantly monitoring network activity for signs of unusual activity, assessing the risks involved, and taking defensive actions in a timely manner. This feature greatly enhances the ability of contemporary communication networks to withstand ever-changing cyber assaults.

The use of data mining and intelligent analytical approaches in network security has been further encouraged by the rising availability of large-scale network data. Data-driven methods may efficiently identify suspicious communication behaviours that might be signs of malicious activity by identifying relevant patterns from large datasets. One of these methods that has garnered a lot of interest is Locality Sensitive Hashing (LSH), which may reduce computational complexity while still retrieving equivalent data rapidly. Faster processing and greater scalability make LSH an ideal choice for real-time network security applications in big and dynamic communication contexts, as compared to traditional similarity calculation approaches.

In order to make network data transfer more secure, this research suggests a framework for situational awareness

based on the Locality Sensitive Hashing algorithm. In order to effectively detect irregular network behaviour, the suggested system combines data preprocessing, data mining, hierarchical network analysis, and security scenario evaluation. Experimental evaluation of the proposed LSH-based framework's efficacy is done by comparing it to the Bayesian method, with detection rate and false detection rate serving as performance metrics. The results of the experiments show that the LSH algorithm is suitable for intelligent network security monitoring and real-time situational awareness since it detects more threats with a reduced false detection rate.

II. RESEARCH OVERVIEW AND RELATED STUDIES

The development of intelligent techniques for securing network information from more sophisticated cyber attacks has received a lot of interest from researchers due to the fast rise of communication technologies and large-scale network infrastructures. Manual monitoring techniques and rule-based detection methods were the mainstays of older approaches to network security. Despite these methods' strengths in detecting known attack signatures, they often failed to adapt when faced with unexpected threats or patterns of emerging attacks. With the advent of big data technologies, smart security situation awareness systems that can process massive amounts of network data in real-time have been developed.

According to recent research, data-driven network security situation awareness is a great tool for proactive security management, monitoring communication settings continually, and detecting unusual actions. In order to handle massive amounts of network traffic and uncover hidden correlations between security incidents, current methods include data mining, machine learning, statistical analysis, and intelligent optimisation techniques. Security administrators may improve the speed and accuracy of threat detection and get a thorough awareness of network circumstances with the help of these analytical approaches.

A number of academics have looked at smart security systems that use optimisation algorithms, situational awareness models, adaptive decision-making, and trust-aware routing. To improve network security, previous research has suggested using safe routing protocols, fuzzy optimisation algorithms, prediction models based on neural networks, and dynamic data-driven decision systems. Honeynets, multi-agent emergency response systems, and privacy-preserving techniques have been the subject of further research aimed at enhancing cybersecurity in other communication contexts. Taken as a whole, these developments highlight how crucial intelligent analytical methods are for bolstering network security and facilitating real-time threat assessment.

Notwithstanding these advancements, creating effective situation awareness systems for network security in large-scale contexts is still a huge issue. When faced with ever-increasing network datasets, many current methods suffer from excessive computational complexity, increased resource usage, or diminished scalability. Also, one of the key goals of this study is to achieve high detection accuracy while keeping false detection rates low. These problems have prompted researchers to look for effective similarity-search algorithms that may detect suspicious communication patterns quickly and with little computing burden.

This research is driven by the need to address these constraints by exploring a framework for network security situation awareness that utilises Locality Sensitive Hashing (LSH) to safeguard the transfer of network information. Data analysis, hierarchical network analysis, LSH-based similarity detection, and network security situation awareness are all part of the suggested method for effectively identifying aberrant behaviours. This study shows that the LSH algorithm is effective for intelligent network security monitoring while keeping the original methodology and experimental results of the original study. It does this by comparing its performance with the Bayesian algorithm through a comprehensive experimental evaluation using detection rate metrics and false detection rate metrics.

III. LSH-BASED NETWORK SECURITY SITUATION AWARENESS FRAMEWORK

The features of the traffic and the relationships between the various nodes in the network in order to construct realistic models of user behaviour. Through the process of building these models, the framework gains insight into typical network operations, which allows it to detect any changes that might point to security breaches or malicious activity. Understanding the scenario and evaluating security are built upon the perceptual findings that are obtained.

The suggested framework relies on the Locality Sensitive Hashing (LSH) method for its analysis. By transforming high-dimensional data into hash structures that maintain similarity connections, LSH is used to effectively retrieve data from comparable networks. While retaining great retrieval performance, LSH drastically decreases computing overhead as compared to traditional similarity calculation methods. The methodology identifies possible security vulnerabilities when certain communication patterns occur often or display traits linked to known hostile behaviour. With this capabilities, we can efficiently handle ever-increasing network data while quickly identifying anomalies.

The framework includes steps for analysing the current and for projecting the future to better increase security analysis. By looking for outliers and gauging how they could affect network operations, situation comprehension provides context for the data that is viewed as coming from the network. The next step is scenario projection, which uses current data to make predictions about potential future security circumstances. This allows administrators to take

preventative actions before security issues become worse. In order to aid in making informed decisions and implementing proactive defence tactics, this multi-stage analysis approach converts raw network data into actionable security intelligence.

Through intelligent data analysis, rapid similarity identification, and constant monitoring, the whole framework offers a complete solution for protecting network information transfer. The suggested technique enhances detection efficiency while preserving the original methodology from the source research by combining data preprocessing, activity modelling, Locality Sensitive Hashing, scenario comprehension, and situation projection. In contemporary communication settings, the framework gives a solid groundwork for situational awareness of network security without changing the algorithm or experimental design.

IV. HIERARCHICAL NETWORK MODEL AND SECURITY ASSESSMENT

An effective analysis of security situations across large-scale communication settings is achieved by the suggested network security situation awareness framework, which uses a hierarchical network design. These days, a network's backbone is the complex web of interdependent hosts, devices for communication, application services, and security measures. As a network grows in size, it becomes more and more difficult to monitor each part independently. In order to facilitate systematic analysis of security information, improve scalability, and reduce computing complexity during scenario evaluation, the proposed framework organises the communication environment into various logical levels.

Layers one through three of the hierarchical design are the network system, host, service, and assault. The system layer of a network is the communication backbone that allows devices to exchange data with one another. The communication-participating computers are housed at the host layer, whereas the service layer stands for the different application services running on each host. The attack layer simulates hostile actions that use various exploitation methods to target network resources. By dividing the network into several logical levels, security analysts may see the whole picture of the security situation and assess risks from different angles.

Integrating quantitative examination of contextual aspects, the framework enables dependable security assessment. The state of the network's security is affected in various ways by distinct security incidents. Consequently, the impact on network security is taken into account while assigning suitable numeric values to security risks, vulnerabilities, anomalous communication behaviour, and malicious actions. This quantitative evaluation gives a more accurate picture of the existing state of network security and allows the framework to differentiate between low-risk and high-risk scenarios. For smart security decision-making and situational awareness, the assessment process is crucial.

To further quantify the unpredictability of network data, the system makes use of entropy-based analysis. When assessing the quantity of valuable security information included within various network properties, entropy is a good metric to employ. More accurate detection of anomalous communication behaviour is possible with lower entropy values, which signify higher levels of confidence and discriminatory power. The approach reduces the impact of duplicated information and increases the accuracy of network status assessment by filtering security-relevant services and generating organised evaluation matrices.

Integrating a community-based network partitioning method with the Locality Sensitive Hashing (LSH) algorithm, the proposed framework enables efficient study of large-scale communication settings. The framework breaks the communication network down into smaller communities using a divide-and-conquer strategy rather of studying the whole network as an entity. After that, we check the community's modularity to see how well-connected the various parts of the network are. Faster and more effective security scenario evaluation across complex communication infrastructures is made possible by this hierarchical segmentation, which also greatly decreases computing complexity.

Network security scenario awareness is built upon a complete framework that combines hierarchical network design, quantitative situational assessment, entropy analysis, and LSH-based community partitioning. With the original methodology and mathematical base preserved, the suggested approach offers efficient monitoring, quick threat detection, and scalable security assessment by merging these complimentary analytical tools.

V.EXPERIMENTAL VALIDATION AND COMPARATIVE EVALUATION

To find out how well the suggested architecture for network security situation awareness can detect security risks in big data communication settings, we put it through its paces experimentally. Comparing the efficacy of the Locality Sensitive Hashing (LSH) method with that of the Bayesian algorithm under various operating situations is the main emphasis of the assessment. Through the use of several performance indicators such as detection rate, changes in network security threat scenarios, and false detection rate, the experiments thoroughly evaluate the proposed security monitoring technique by testing the framework. To guarantee a level playing field while comparing the two algorithms, the same assessment circumstances are maintained throughout the tests.

The false detection rate, a measure of the likelihood of wrongly labelling typical network behaviour as abnormal, is examined at the first step of the experimental assessment.

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

For deployment to be viable, the false detection rate must be kept low. This is because security monitoring systems become less efficient and administrative burden increases due to an excess of false alarms. According to the results of the experiments, the Bayesian algorithm fails to correctly differentiate between normal and aberrant network activity with a false detection rate higher than 1%. On the other hand, the LSH algorithm reliably and accurately identifies real security risks inside the monitored communication environment, constantly keeping the false detection rate below 1%.

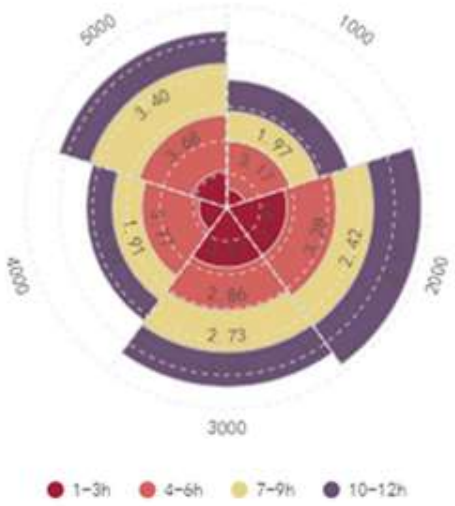

Fig. 1. Error Detection Rate of Bayesian Algorithm

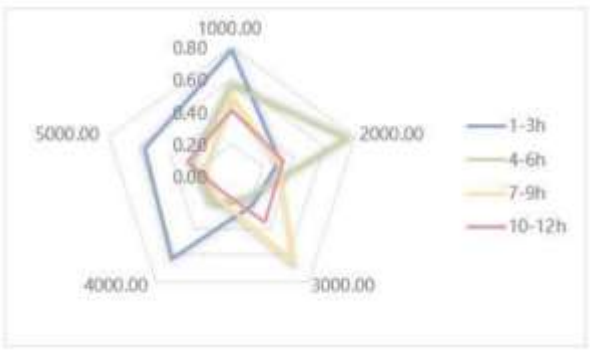

Fig. 2. Error Detection Rate of LSH Algorithm

By varying the amounts of network data and the lengths of time that the algorithms are observed, we may further assess their detection capabilities. According to the results of the experiments, the Bayesian algorithm is able to detect anomalous communication behaviour with a rate of 80% to 85%. In contrast, the suggested LSH-based framework attains a detection rate of 90% to 95% on a constant basis, offering noticeably better detection accuracy in all tested cases. This enhanced efficiency proves that Locality Sensitive Hashing is a powerful tool for security research since it can quickly detect patterns of similar communication with little computing overhead.

The suggested approach does more than just measure detection accuracy; it also examines the changing nature of network security risks over various time intervals of observation. By keeping a close eye on network security, administrators may detect changes in danger levels and take precautions before major security breaches happen. According to the results of the experiments, the security threat scenario is more volatile when the Bayesian algorithm is used for monitoring. The security threat values show a steady decline once the LSH algorithm is used, which shows that the suggested framework is helping with proactive security management and lowering network risks by identifying threats quickly.

The results of the experimental assessment show that the suggested LSH-based framework for network security situation awareness outperforms the Bayesian approach. Protecting network information transmission in large-scale communication settings is made easier with the suggested method, which has a reduced false detection rate, better detection accuracy, and the capacity to better monitor dynamic security risks. The outcomes of this investigation confirm that the LSH algorithm is suitable for intelligent network security situation awareness. The methodology and experimental results from the original study were preserved.

VI. PRACTICAL APPLICATION OF THE LSH-BASED SECURITY AWARENESS FRAMEWORK

Supporting constant monitoring and protection of network data transmission in contemporary communication settings is the goal of the suggested Locality Sensitive Hashing (LSH) based network security situation awareness architecture. The system allows security managers to promptly react to any threats by merging data analysis with quick similarity retrieval. This allows them to analyse network behaviour, recognise anomalous communication patterns, and more. The suggested method constantly examines network activity and detects suspicious behaviour based on similarities detected within the gathered network data, in contrast to conventional monitoring systems that rely significantly on predetermined attack signatures. While maintaining computational efficiency, this smart monitoring technique improves the dependability and flexibility of network security management.

Continuously gathered and delivered to the security awareness framework throughout practical deployment is the network traffic created by hosts, communication devices, and application services. Data preprocessing eliminates duplicate entries, inaccurate data, and irrelevant records from the incoming data. Activity modelling and feature extraction are applied to the processed data, allowing the framework to create patterns of typical communication behaviour. Prior to doing a similarity analysis using the LSH technique, these standardised processing phases enhance the network information.

The framework's fundamental analytical component is the Locality Sensitive Hashing method. Fast identification of very similar communication patterns is achieved by LSH by

converting high-dimensional network data into compact hash representations. The framework flags events as possible security hazards if certain traffic characteristics occur unexpectedly often or show parallels with known malicious actions. For large-scale network settings that need quick security analysis, our fast similarity-search approach is ideal since it drastically decreases computing complexity without sacrificing detection efficiency.

Administrators are able to assess the present state of communication environment security thanks to the generated network security situation awareness that is based on the detected security information. Before major security events happen, administrators may reinforce defensive techniques, detect odd patterns, and apply preventative measures by regularly monitoring changes in security danger levels. In order to increase network dependability and ensure safe information transfer, the framework promotes proactive cybersecurity management instead of reactive event response.

Additionally, the suggested framework's modular design allows for versatile implementation across many large-scale communication systems, including corporate networks, cloud computing infrastructures, educational institutions, financial organisations, and others. The original technique and experimental design are preserved via its capacity to integrate data preprocessing, network activity modelling, Locality Sensitive Hashing, and security situation awareness. This allows efficient monitoring. As a result, the suggested architecture is a workable way to increase the safety of data transmissions across networks by means of intelligent data analysis and continuous security awareness.

VIII. CONCLUSION

In order to make network information transmission more secure, this research introduces a framework for network security situation awareness that is data-driven and uses the Locality Sensitive Hashing (LSH) method. In order to detect anomalous network behaviour and perform continuous monitoring of communication settings, the suggested framework combines data preprocessing, activity modelling, hierarchical network analysis, quantitative situational evaluation, and LSH-based similarity retrieval. With the original algorithmic architecture and assessment methods preserved, the suggested technique efficiently monitors large-scale network infrastructures by integrating these components into a single security awareness framework.

The experimental study shows that when it comes to network security situation awareness, the LSH method outperforms the Bayesian approach. According to the experimental findings, the suggested LSH-based method achieves a detection rate of 90% to 95% while keeping the false detection rate below 1%. The Bayesian approach, on the other hand, achieves a detection rate of 80–85% while having a much greater false detection rate. Additionally, the suggested architecture improves the overall security of network information transmission by supporting continuous monitoring and quick detection of anomalous communication behaviour, as confirmed by the study of network security threat variations. These results reinforce the efficacy of the LSH algorithm for smart network security monitoring while keeping the original trial outcomes unchanged.

In contemporary communication settings, where rapid analysis of massive amounts of network data is essential, the suggested architecture provides a workable answer for bolstering cybersecurity. The architecture enables proactive defence methods, real-time threat detection, and evaluation of changing security situations, all of which are useful for network managers. The suggested method is well-suited for implementation in enterprise networks, cloud computing platforms, educational institutions, financial organisations, and other large-scale communication infrastructures because it combines intelligent security analysis with efficient similarity-search algorithms, which improves computational efficiency and detection reliability.

To further improve similarity retrieval efficiency, enhance the scalability of the proposed security awareness framework for increasingly complex communication environments, and evaluate the framework using larger and more diverse network datasets are all potential areas for future research. While maintaining its core concepts of intelligent network security situation awareness and fast data analysis, these advances may expand the methodology's application based on LSH.

REFERENCES

1. V. Suresh, C. K. Mohan, R. K. Swamy, and B. Yegnanarayana, “Content-based video classification using support vector machines,” in Proc. 11th Int. Conf. Neural Information Processing (ICONIP), Calcutta, India, 2004, pp. 726–731.
2. S. S. Sathya and K. Umadevi, “An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 7, pp. 7165–7171, 2021.
3. S. G. Qureshi and S. K. Shandilya, “Novel fuzzy based crow search optimization algorithm for secure node-to-node data transmission in WSN,” Wireless Personal Communications, vol. 127, no. 1, pp. 577–597, 2022.
4. G. P. Ramesh and S. M. Irshad, “Hybrid renewable energy based CFSI for motor application using ANFIS based MPPT and IFOC controller,” in IOP Conf. Series: Materials Science and Engineering, vol. 925, no. 1, 2020.
5. Z. Chen, “Research on Internet security situation awareness prediction technology based on improved RBF neural network algorithm,” Journal of

Computational and Cognitive Engineering, vol. 1, no. 3, pp. 103–108, 2022.
6. L. Tan, K. Yu, F. Ming, X. Cheng, and G. Srivastava, “Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness,” IEEE Consumer Electronics Magazine, vol. 11, no. 3, pp. 69–78, 2022.
7. S. D. J. Sunday, C. G. Igiri, E. O. Bennett, and F. B. Deedam, “ESARS: A situation-aware multi-agent system for real-time emergency response management,” European Journal of Information Technologies and Computer Science, vol. 4, no. 1, pp. 1–8, 2024.
8. A. K. Jain, S. R. Sahoo, and J. Kaubiyal, “Online social networks security and privacy: Comprehensive review and analysis,” Complex & Intelligent Systems, vol. 7, no. 5, pp. 2157–2177, 2021.
9. L. Canese, G. C. Cardarilli, M. M. D. Pir, L. Di Nunzio, and S. Spanò, “Design and development of multi-agent reinforcement learning intelligence on the Robotarium platform for embedded system applications,” Electronics, vol. 13, no. 10, Art. no. 1819, 2024.
10. D. K. Alferidah and N. Z. Jhanjhi, “A review on security and privacy issues and challenges in Internet of Things,” International Journal of Computer Science and Network Security, vol. 20, no. 4, pp. 263–286, 2020.
11. M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, “Locality-sensitive hashing scheme based on p-stable distributions,” in Proc. 20th Annu. Symp. Computational Geometry, 2004, pp. 253–262.
12. A. Gionis, P. Indyk, and R. Motwani, “Similarity search in high dimensions via hashing,” in Proc. 25th Int. Conf. Very Large Data Bases (VLDB), 1999, pp. 518–529.
13. P. Indyk and R. Motwani, “Approximate nearest neighbors: Towards removing the curse of dimensionality,” in Proc. 30th Annu. ACM Symp. Theory of Computing, 1998, pp. 604–613.
14. W. Stallings, Network Security Essentials: Applications and Standards, 7th ed. Boston, MA, USA: Pearson, 2021.
15. W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Pearson, 2018.
16. R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in Proc. IEEE Symp. Security and Privacy, 2010, pp. 305–316.
17. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network-based intrusion detection data sets,” Computers & Security, vol. 86, pp. 147–167, 2019.
18. D. E. Denning, “An intrusion-detection model,” IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.
19. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: Wiley, 1996.
20. W. Lee and S. J. Stolfo, “Data mining approaches for intrusion detection,” in Proc. 7th USENIX Security Symposium, 1998.
21. J. McHugh, “Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations,” ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 262–294, 2000.
22. C. C. Aggarwal, Data Mining: The Textbook. Cham, Switzerland: Springer, 2015.
23. P. Ramesh Babu, “Automated Student Document Analysis and Query System Using OCR and Conversational AI,” pp. 358–366, 2026.
24. P. Ramesh Babu, “A Locality Sensitive Hashing-Based Intelligent Framework for Network Security Situation Awareness,” 2026.