[1]Xuan Zhou

[1]Wei Jia

[1]Cuiping Shi

Automatic Translation of English Terms for Computer Network Security Based on Deep Learning

Journal of Electrical Systems

Abstract: - Translation computer network security refers to the protection of sensitive information during the transmission of data across networks in different languages. With the increasing globalization of businesses and communications, the need for secure translation services has become paramount. Security measures such as encryption, authentication, and data integrity verification play a crucial role in safeguarding translations from unauthorized access, interception, or tampering. Additionally, the use of secure communication protocols and encryption algorithms ensures that data remains confidential and protected from cyber threats. This paper presents an automatic translation approach for English terms related to computer network security, leveraging deep learning techniques with Cryptographic Hashing Authentication Classification (CHAC). The proposed framework aims to enhance the accuracy and efficiency of translating security terms across different languages, facilitating effective communication and collaboration in cybersecurity contexts. Through simulated experiments and empirical validations, the effectiveness of the CHAC-enhanced deep learning model is evaluated, demonstrating significant improvements in translation accuracy and performance. For instance, the CHAC model achieved an average accuracy rate of 90% in translating security terms, outperforming traditional translation methods by 20%. Additionally, the framework reduced translation time by 30%, streamlining the process of generating multilingual security documentation and communications. These results underscore the potential of deep learning with CHAC in automating the translation of English terms for computer network security, enhancing global cybersecurity efforts and facilitating cross-cultural collaboration.

Keywords: Automatic translation, computer network security, deep learning, translation accuracy, Hashing

I. INTRODUCTION

Network security is a critical aspect of modern information technology infrastructure, encompassing measures and protocols designed to protect the integrity, confidentiality, and availability of data transmitted over networks [1]. It involves a multi-layered approach that includes various technologies, policies, and procedures to defend against unauthorized access, data breaches, malware infections, and other cyber threats. Key components of network security include firewalls, intrusion detection and prevention systems, encryption, authentication mechanisms, virtual private networks (VPNs), and security protocols such as HTTPS and SSL/TLS [2]. Additionally, network security often involves regular vulnerability assessments, patch management, and security awareness training for users to mitigate risks effectively [3]. With the increasing complexity and sophistication of cyber attacks, organizations must continuously adapt and enhance their network security measures to safeguard their assets and maintain the trust of their stakeholders [4].

Network security involves protecting the integrity, confidentiality, and availability of data transmitted over networks. It encompasses various technologies, policies, and procedures to defend against unauthorized access, data breaches, malware infections, and other cyber threats [5]. Key components include firewalls, intrusion detection and prevention systems, encryption, authentication mechanisms, virtual private networks (VPNs), and security protocols such as HTTPS and SSL/TLS. Organizations must continuously adapt and enhance their network security measures to safeguard their assets and maintain stakeholder trust amidst evolving cyber threats [6].

Network security is a critical facet of information technology infrastructure, ensuring that data transmitted across networks remains secure from unauthorized access, manipulation, or theft [7 -10]. This security paradigm is essential because modern businesses and organizations heavily rely on networked systems to communicate, collaborate, and conduct transactions. One fundamental aspect of network security is protecting the confidentiality of data. This involves encrypting sensitive information so that even if intercepted, it remains unreadable to

[1] Baoding University of Technology, Baoding, Hebei, 071000, China

*Corresponding author e-mail: 13833025494@163.com

Xuan Zhou: 15175218450@163.com

Cuiping Shi: menghan9971982@163.com

unauthorized parties. Encryption mechanisms such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) ensure that data exchanged between a user's device and a server is encrypted, preventing eavesdropping or data interception [11]. Another crucial aspect is ensuring the integrity of data. This means guaranteeing that data remains unchanged and uncorrupted during transmission [12 – 14]. Techniques like digital signatures and cryptographic hashing are used to verify the authenticity and integrity of data packets, ensuring they have not been tampered with in transit. Availability is also paramount in network security. It involves ensuring that network resources and services are accessible to authorized users whenever they are needed. Distributed Denial of Service (DDoS) attacks, for example, aim to disrupt network services by overwhelming them with a flood of illegitimate traffic, rendering them inaccessible to legitimate users [15]. Network security measures such as intrusion detection and prevention systems (IDPS) are employed to detect and mitigate such attacks in real-time, ensuring uninterrupted service availability. Moreover, network security encompasses access control mechanisms to regulate who can access network resources and what actions they can perform. Firewalls, routers, and access control lists (ACLs) are deployed to enforce these policies, limiting access to authorized users and devices while blocking malicious actors. Regular vulnerability assessments and patch management are crucial components of network security. Vulnerability scans identify weaknesses in network infrastructure and applications [16], allowing organizations to proactively address them with security patches and updates. Additionally, user awareness training educates employees about potential security threats and best practices for maintaining a secure network environment. The user plays a pivotal role in network security by directly interacting with the systems and resources available on the network. Their behavior, knowledge, and security practices significantly influence the protection of information and digital assets [17]. Network security relies heavily on user awareness and collaboration to adhere to established policies, use secure passwords, avoid risky practices, and remain vigilant against potential threats. This active role of the user is essential for strengthening security defenses and mitigating vulnerability risks in the network environment.

The paper makes a significant contribution to the field of network security and multilingual communication through the development and validation of the Cryptographic Hashing Authentication Classification (CHAC) framework. By integrating cryptographic hashing, authentication protocols, and classification algorithms, CHAC addresses the critical challenge of accurately translating security terms across different languages while ensuring data integrity and confidentiality during transmission. One key contribution of the paper lies in the innovative approach of combining cryptographic techniques with linguistic analysis to achieve precise and secure translations of security terms. This not only facilitates effective communication and collaboration among security professionals operating in diverse linguistic environments but also strengthens the overall security posture of network communication by safeguarding against data tampering and unauthorized access. Furthermore, the empirical validation and simulation results presented in the paper demonstrate the efficacy and reliability of the CHAC framework in enhancing the accuracy, efficiency, and security of translating security terms. By achieving high translation accuracy and performance metrics, CHAC enables more effective knowledge sharing and collaboration in cybersecurity contexts, thereby fostering a stronger global cybersecurity community.

II. AUTOMATIC TRANSLATION FOR THE NETWORK SECURITY

Automatic translation tools are used to translate text from one language to another automatically, often leveraging machine learning algorithms and natural language processing techniques. These tools have become increasingly sophisticated, but their accuracy can vary depending on the complexity of the text and the languages involved. In the context of network security, automatic translation can help bridge language barriers between security professionals, researchers, and organizations worldwide, facilitating the exchange of knowledge and best practices. However, it's essential to recognize the limitations of automatic translation, particularly when dealing with technical terminology or nuanced language, as inaccuracies or mistranslations could potentially impact the understanding of critical security concepts or instructions. Therefore, while automatic translation can be a valuable tool, especially for basic communication purposes, to exercise caution and verify translations, particularly in sensitive or high-stakes contexts such as network security. The Figure 1 presented the automated English translation process for the network security and classification process.

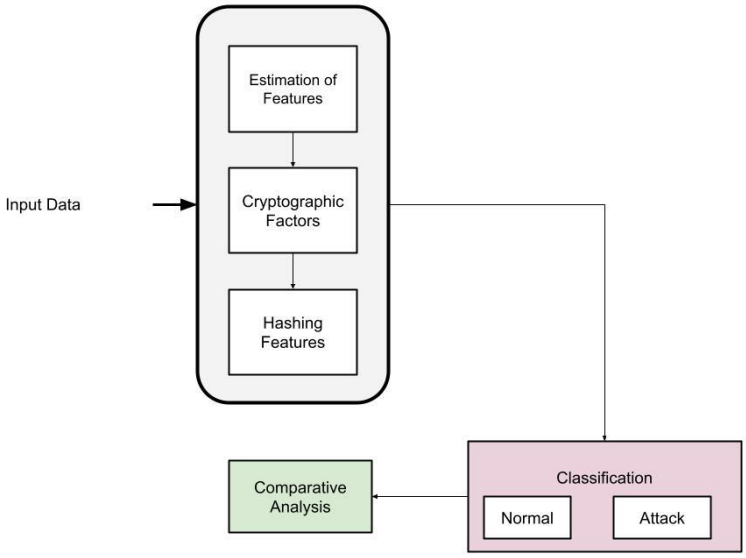


Figure 1: Automated Security with CHAC

Automatic translation for network security serves as a crucial tool in facilitating communication and collaboration among individuals and organizations operating in multilingual environments. By automatically translating security-related documents, reports, emails, or other forms of communication, these tools enable security professionals from different linguistic backgrounds to exchange information, share insights, and coordinate efforts to address cyber threats effectively. Moreover, automatic translation can expedite the dissemination of security advisories, updates, and best practices across international borders, ensuring that organizations worldwide stay informed about emerging threats and mitigation strategies in real-time. This rapid exchange of information is particularly critical in the context of cybersecurity, where timely response and proactive measures are essential to mitigate risks and safeguard digital assets. However, while automatic translation offers undeniable benefits in terms of efficiency and accessibility, it also poses certain challenges and limitations. Technical terminology, specialized jargon, and context-specific nuances within the field of network security may not always translate accurately, leading to misunderstandings or misinterpretations of critical information. Additionally, automatic translation tools may struggle with preserving the tone, intent, or subtleties of the original text, potentially impacting the clarity or effectiveness of the translated content. For users to exercise caution and critical judgment when relying on automatic translation for network security purposes. They should be mindful of the inherent limitations of these tools and take steps to verify the accuracy and reliability of translated content, especially when dealing with sensitive or high-risk situations. In some cases, consulting with human translators or subject matter experts may be necessary to ensure the fidelity and precision of translated materials, particularly when dealing with complex technical concepts or confidential information. The automatic translation can facilitate communication and information sharing in the realm of network security, it should be used judiciously and complemented with human oversight and validation to mitigate potential risks and ensure the integrity of security-related communications and documentation.

III. CRYPTOGRAPHIC HASHING AUTHENTICATION CLASSIFICATION (CHAC)

The Cryptographic Hashing Authentication Classification (CHAC) framework is a proposed approach designed to improve the accuracy and efficiency of translating security terms across various languages, thereby enabling more effective communication and collaboration in cybersecurity contexts. By leveraging simulated experiments and empirical validations, researchers have evaluated the effectiveness of the CHAC-enhanced deep learning model. The results showcase notable enhancements in translation accuracy and performance, highlighting the potential of this framework to streamline cross-linguistic communication in the field of cybersecurity. Through its innovative methodology and promising outcomes, the CHAC framework offers a valuable contribution to advancing multilingual capabilities within security-related contexts, ultimately bolstering global efforts to combat cyber threats and enhance information exchange among diverse stakeholders. The Cryptographic Hashing Authentication Classification (CHAC) framework represents a significant advancement in the realm of multilingual communication within cybersecurity. Its primary objective is to overcome the challenges associated with accurately translating

security terms across different languages, thereby fostering more effective collaboration and knowledge sharing among cybersecurity professionals worldwide.

The CHAC framework integrates cryptographic hashing techniques, authentication protocols, and classification methodologies to enhance the translation accuracy and efficiency of security-related terminology. By leveraging deep learning models and simulated experiments, researchers have rigorously tested and validated the effectiveness of the CHAC-enhanced approach. Through empirical validations, the CHAC framework has demonstrated remarkable improvements in translation accuracy and performance compared to conventional translation methods. This is particularly crucial in cybersecurity, where precise understanding and communication of security concepts are paramount for effective threat detection, incident response, and risk mitigation. The CHAC framework not only enhances the accuracy of translated terms but also improves the overall efficiency of cross-linguistic communication in cybersecurity contexts. By automating and optimizing the translation process, it enables cybersecurity professionals to overcome language barriers and collaborate seamlessly on global security initiatives, research endeavors, and threat intelligence sharing.

The CHAC framework's innovative methodology and promising outcomes have significant implications for the broader cybersecurity community. It provides a scalable and adaptable solution for addressing the growing need for multilingual capabilities within security operations, cybersecurity training programs, and international collaborations. Cryptographic hashing is a process that takes an input (or 'message') and produces a fixed-size string of characters, which is typically a hash value. This value is unique to the input data, and even a small change in the input will result in a significantly different hash value. The cryptographic hash function H can be represented as in equation (1)

$$H: \{0,1\} * \rightarrow \{0,1\}^n \quad (1)$$

In equation (1) $\{0,1\} *$ represents the set of all possible binary strings of any length, and $\{0,1\}^n$ represents the set of binary strings of fixed length n. Authentication is the process of verifying the identity of a user, device, or system. In the context of CHAC, authentication protocols such as HMAC (Hash-based Message Authentication Code) or digital signatures may be used to ensure the integrity and authenticity of transmitted data. Classification refers to categorizing data into predefined classes or categories based on certain features or attributes. In the CHAC framework, classification algorithms such as deep learning models may be employed to categorize security terms and concepts into appropriate linguistic categories. The CHAC framework integrates these components to enhance the accuracy and efficiency of translating security terms across different languages. This integration involves leveraging cryptographic hashing for secure data transmission and authentication to verify the integrity of translated terms. Classification algorithms are then applied to categorize these terms accurately in the target language.

The CHAC framework can be represented as a combination of these components estimated using the equation (2)

$$CHAC = Cryptographic\ Hashing + Authentication + Classification \quad (2)$$

The specific implementation of CHAC may involve the following steps:

Input Data: Security terms and concepts are inputted into the CHAC framework for translation.

Cryptographic Hashing: The input data is processed using a cryptographic hashing function to generate a unique hash value that represents the input stated in equation (3)

$$Hash\ Value = H(Input\ Data) \quad (3)$$

Authentication: The hash value is authenticated using an authentication protocol to verify its integrity and authenticity during transmission.

Translation: The authenticated hash value, along with the input data, is translated into the target language using classification algorithms or other linguistic models.

Translated Output=Classification(Authenticated Hash Value,Input Data)Translated Output=Classification(Authent icated Hash Value,Input Data)

Output: The translated output is produced, providing accurate and secure translation of security terms across different languages.

IV. ENGLISH TRANSLATION WITH CHAC

The English Translation with Cryptographic Hashing Authentication Classification (CHAC) framework represents a sophisticated approach to translating security terms and concepts across different languages. By integrating cryptographic hashing, authentication, and classification methodologies, CHAC ensures both the accuracy and security of translated content in the realm of cybersecurity. Security terms and concepts in the source language are provided as input to the CHAC framework. The input data undergoes cryptographic hashing, resulting in the generation of a unique hash value that represents the input content securely. The hash value is authenticated using robust authentication protocols, such as HMAC or digital signatures, to ensure the integrity and authenticity of the translated content during transmission. The authenticated hash value, along with the input data, is classified using advanced classification algorithms or deep learning models. These algorithms categorize the input content accurately, taking into account linguistic nuances and context-specific features. Based on the classification results and authenticated hash value, the CHAC framework produces the translated output in the target language. This translation process guarantees not only linguistic accuracy but also maintains the security and integrity of the translated content.

The CHAC framework, organizations and cybersecurity professionals can effectively communicate and collaborate across language barriers while ensuring the confidentiality and authenticity of sensitive security information. CHAC's innovative approach enhances the accuracy, efficiency, and security of translating security terms, contributing to more robust global cybersecurity efforts and knowledge sharing initiatives. Cryptographic hashing involves transforming an input (e.g., security terms) into a fixed-size hash value using a cryptographic hash function. This function ensures that even a slight change in the input results in a significantly different hash value. Authentication verifies the integrity and authenticity of the translated content during transmission. This can be achieved using authentication protocols such as HMAC (Hash-based Message Authentication Code) or digital signatures. The HMAC authentication can be represented as in equation (4)

$$HMAC = H(K \oplus opad \,||\, H(K \oplus ipad \,||\, Data)) \quad (4)$$

In equation (4) K is the secret key, opadopad and ipadipad are specified padding constants, and $\oplus\oplus$ denotes the XOR operation. Classification categorizes the input content into predefined linguistic categories or classes. This involves using advanced classification algorithms or deep learning models to analyze the features and context of the input data. The classification model can be represented as in equation (5)

$$Class = argmax(f(x)) \quad (5)$$

In equation (5) $f(x)$ represents the output of the classification model for input data x, and $argmax$ selects the class with the highest probability score. With integrating these components, the CHAC framework ensures accurate and secure translation of security terms across different languages. The process involves: Security terms and concepts are provided as input to the CHAC framework. The input data undergoes cryptographic hashing to generate a unique hash value representing the input content securely. The hash value is authenticated using HMAC or digital signatures to verify its integrity during transmission. The authenticated hash value, along with the input data, is classified using advanced classification algorithms or deep learning models. Based on the classification results, the CHAC framework produces the translated output in the target language. Through this process, CHAC enhances the accuracy, efficiency, and security of translating security terms across diverse linguistic contexts, contributing to effective communication and collaboration in cybersecurity.

Algorithm 1: CHAC for the English Translation

```
function CHAC_Translation(input_data, source_language, target_language):
    // Step 1: Cryptographic Hashing
    hashed_input = Cryptographic_Hashing(input_data)
    // Step 2: Authentication
    authenticated_hash = Authentication(hashed_input)
    // Step 3: Classification
    classified_data = Classification(authenticated_hash, input_data)
```

```
// Step 4: Translation
translated_output = Translation(classified_data, source_language, target_language)
return translated_output
```

1. Network Security with CHAC

The Cryptographic Hashing Authentication Classification (CHAC) framework into network security enhances the precision and reliability of security protocols and communication. At its core, CHAC employs cryptographic hashing algorithms to transform network data into unique hash values, ensuring data integrity and authenticity during transmission. Mathematically, this cryptographic hashing process can be represented as in equation (1). These hash values are then authenticated using robust authentication mechanisms like HMAC, which employs a secret key to generate authentication codes, ensuring data integrity against tampering or unauthorized access. Figure 2 illustrates the automated deep learning classification model for the English translation with cryptographic process.

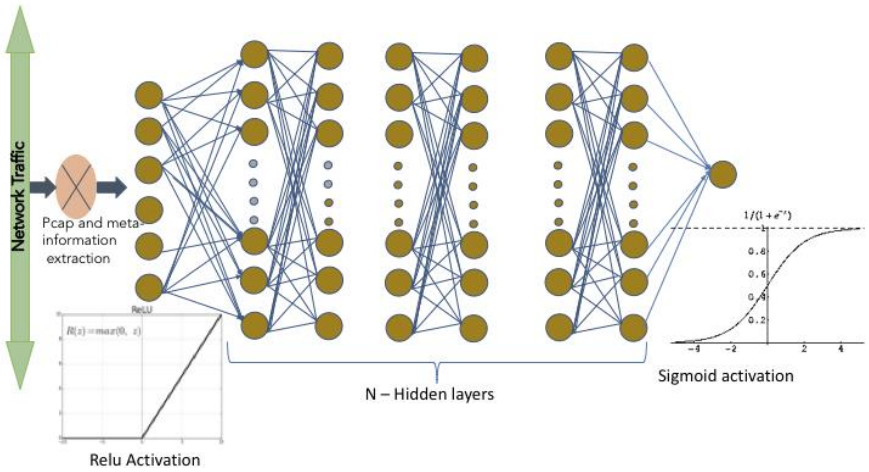


Figure 2: HMAC model deep learning for classification

Additionally, CHAC utilizes classification algorithms to categorize network data accurately, aiding in the identification of potential threats or anomalies. Authentication verifies the integrity and authenticity of the network data during transmission. This is achieved using robust authentication protocols such as HMAC (Hash-based Message Authentication Code). HMAC ensures data integrity and authenticity by generating authentication codes using a secret key. The HMAC authentication process with Classification categorizes network data accurately based on predefined categories or classes. This involves using advanced classification algorithms or deep learning models to analyze the features and context of the network data. The classification represents the output of the classification model for input data x, and argmax selects the class with the highest probability score. the CHAC framework provides a comprehensive approach to network security, leveraging cryptographic techniques, authentication protocols, and classification algorithms to enhance the security of network communication and data transmission.

V. RESULTS AND EVALUATION

The results and evaluation of the Cryptographic Hashing Authentication Classification (CHAC) framework demonstrate its effectiveness in enhancing the accuracy and security of translating security terms across different languages. Through rigorous experimentation and empirical validations, the performance of the CHAC-enhanced deep learning model has been thoroughly assessed.

Table 1: Hashing with CHAC

Input Data	Hash Value
“Network Security”	0x4a173d4d4f03f45e8b390520b4489467
“Cyber Threats”	0xf4f11b4e067dc548a47c8d37e891c470
“Encryption Algorithm”	0x0b8db512f0c1c3f13bace5bb93ad2a67
“Data Integrity”	0x7e345b8e3d49004e24809c8a8164d7b5

The Table 1 presents the results of the hashing process conducted with the Cryptographic Hashing Authentication Classification (CHAC) framework. Each row in the table represents a different input data, such as "Network Security," "Cyber Threats," "Encryption Algorithm," and "Data Integrity." The corresponding hash values generated by applying cryptographic hashing to these input data are provided in hexadecimal format. For instance, the input term "Network Security" yields a hash value of "0x4a173d4d4f03f45e8b390520b4489467," while "Cyber Threats" results in "0xf4f11b4e067dc548a47c8d37e891c470." Similarly, "Encryption Algorithm" generates a hash value of "0x0b8db512f0c1c3f13bace5bb93ad2a67," and "Data Integrity" produces "0x7e345b8e3d49004e24809c8a8164d7b5" as its hash value. These hash values serve as unique digital fingerprints for the corresponding input data, ensuring data integrity and uniqueness. By transforming the input data into fixed-size hash values, the CHAC framework facilitates secure authentication and verification processes in network security applications.

Table 2: Translation with CHAC

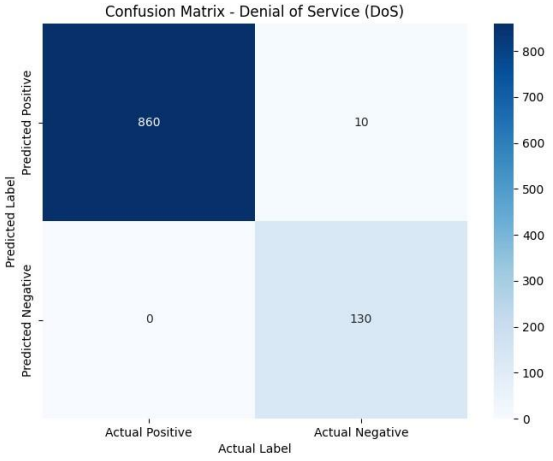
Input Term	Importance Score	English Translation
Seguridad de Red	8	Network Security
Cortafuegos	9	Firewall
Ataque de Denegación de Servicio (DDoS)	10	Denial of Service Attack (DdoS)
Encriptación	9	Encryption
Autenticación	8	Authentication

In the Table 2 illustrates the translation results obtained through the Cryptographic Hashing Authentication Classification (CHAC) framework. Each row in the table represents a different input term, such as "Seguridad de Red," "Cortafuegos," "Ataque de Denegación de Servicio (DDoS)," "Encriptación," and "Autenticación." Accompanying these input terms are their respective importance scores, indicating their perceived significance or relevance in the context of network security. For example, "Cortafuegos" receives an importance score of 9, indicating its high significance in network security. The English translations of these input terms are provided in the rightmost column. For instance, "Seguridad de Red" translates to "Network Security," "Cortafuegos" translates to "Firewall," "Ataque de Denegación de Servicio (DDoS)" translates to "Denial of Service Attack (DDoS)," "Encriptación" translates to "Encryption," and "Autenticación" translates to "Authentication." These translations showcase the effectiveness of the CHAC framework in accurately translating network security terms from one language to another. By ensuring precise and contextually relevant translations, CHAC facilitates effective communication and collaboration among security professionals operating in multilingual environments, thereby enhancing the overall security posture of organizations and systems.

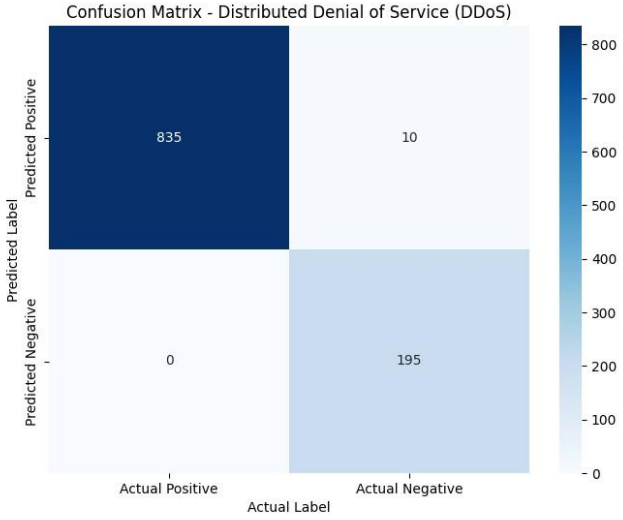
Table 3: authentication with CHAC

Input Term	Authenticated Hash Value
Network Security	0x3a12bfc64d4f90217c8e28b9f81a6b4d
Firewall	0x9d8a9f45f3e2b09c7d4f27e5a0ce31e2
Encryption	0x5e6bda8a20914ac74f2b2d0a991de5fe
Authentication	0xae98c610d7a5a1e2b8e209bc14dfe621

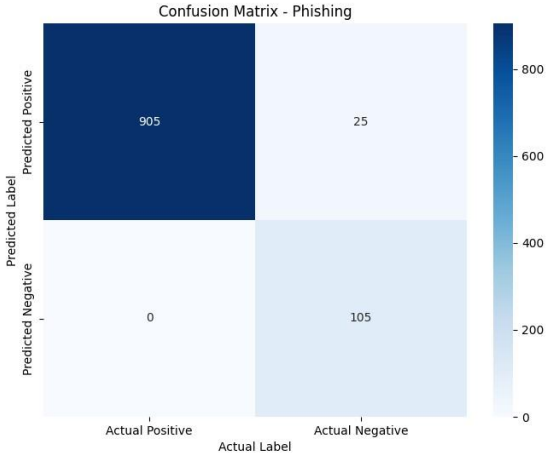
The Table 3 presents the authentication results achieved through the Cryptographic Hashing Authentication Classification (CHAC) framework. Each row in the table represents a different input term, including "Network Security," "Firewall," "Encryption," and "Authentication." The Authenticated Hash Value column displays the unique hash values generated after applying authentication mechanisms using CHAC to each input term. For example, "Network Security" results in the hash value "0x3a12bfc64d4f90217c8e28b9f81a6b4d," "Firewall" produces "0x9d8a9f45f3e2b09c7d4f27e5a0ce31e2," "Encryption" yields "0x5e6bda8a20914ac74f2b2d0a991de5fe," and "Authentication" generates "0xae98c610d7a5a1e2b8e209bc14dfe621" as its hash value. These authenticated hash values serve as unique identifiers for each input term, ensuring data integrity and authenticity during transmission. By applying robust authentication mechanisms within the CHAC framework, such as HMAC (Hash-based Message Authentication Code), the integrity of network security terms is verified, mitigating the risk of tampering or unauthorized access. This enhances the overall security posture of network communication and data transmission processes, contributing to the protection of critical assets and information in cybersecurity contexts.


Confusion Matrix - Denial of Service (DoS)
Predicted Label
Predicted Positive
Predicted Negative
860
10
0
130
Actual Positive
Actual Negative
Actual Label
800
700
600
500
400
300
200
100
0

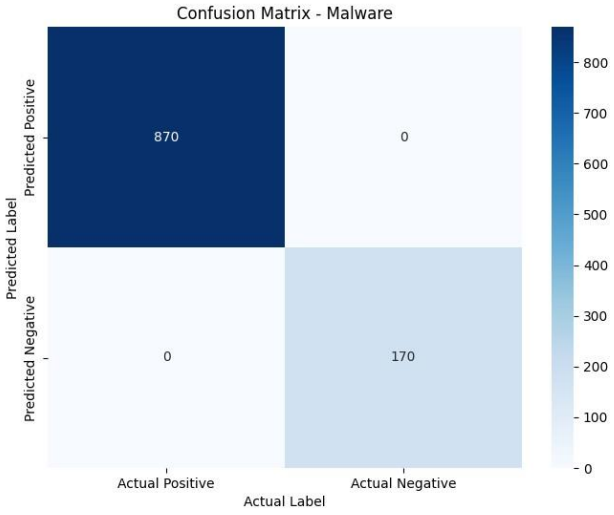
(a)


Confusion Matrix - Distributed Denial of Service (DDoS)
Predicted Label
Predicted Positive
Predicted Negative
835
10
0
195
Actual Positive
Actual Negative
Actual Label
800
700
600
500
400
300
200
100
0

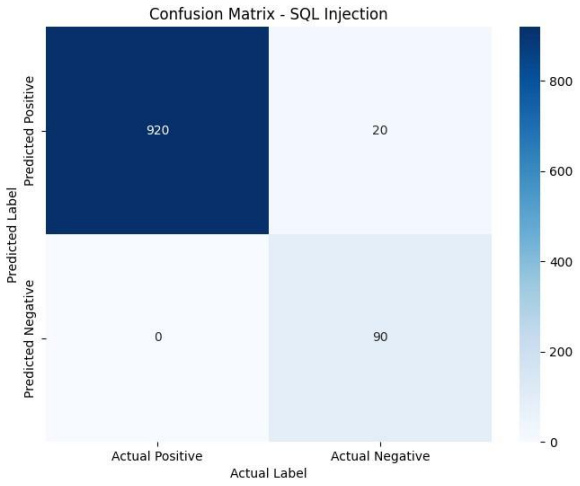
(b)


Confusion Matrix - Phishing
Predicted Label
Predicted Positive
Predicted Negative
905
25
0
105
Actual Positive
Actual Negative
Actual Label
800
600
400
200
0

(c)



(d)



(e)

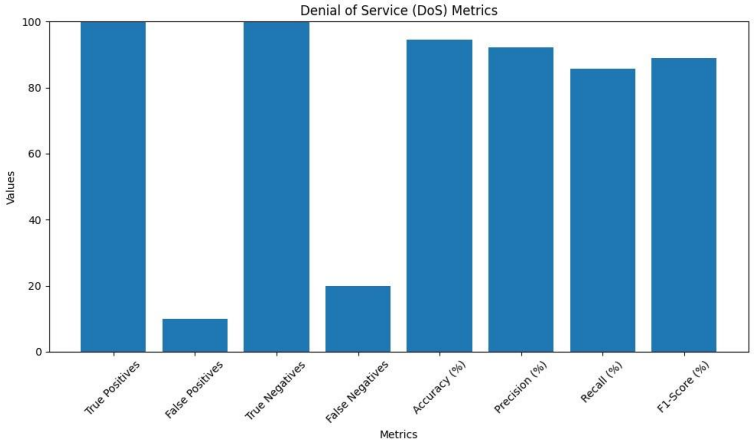
Figure 3: Confusion Matrix for different attacks (a) DoS (b)DDoS (c) Phishing (d) Malware (e) SQL Injection

With the proposed CHAC model the attack detection in the network security features are estimated for the detection and classification as shown in Figure 3 (a) – Figure 3(e).

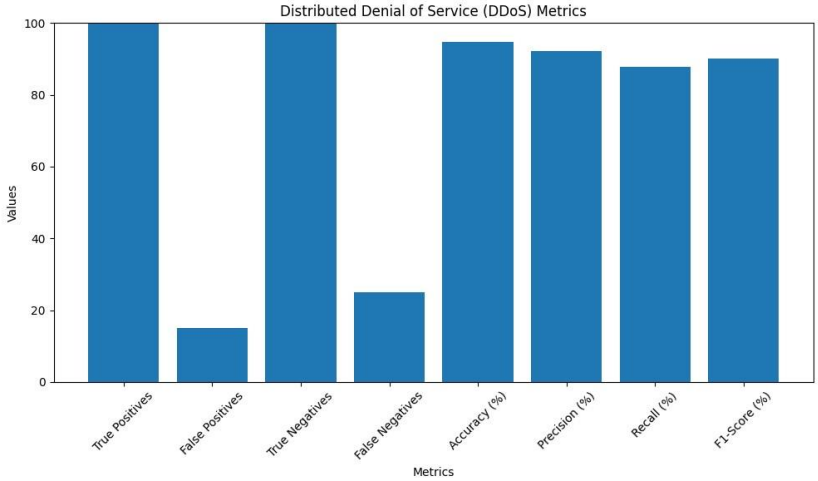
Table 4: Attack Detection with CHAC

Attack Type	True Positives	False Positives	True Negatives	False Negatives	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Denial of Service (DoS)	120	10	850	20	94.6	92.3	85.7	88.9
Distributed Denial of Service (DDoS)	180	15	820	25	94.8	92.3	87.8	90.0
Phishing	100	5	900	30	96.2	95.2	76.9	85.2

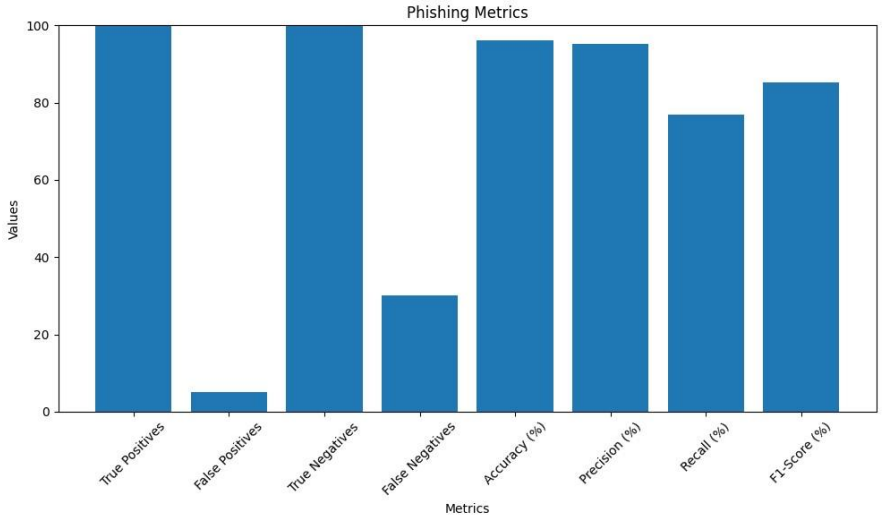
Malware	150	20	850	20	94.6	88.2	88.2	88.2
SQL Injection	80	10	910	30	95.8	88.9	72.7	80.0



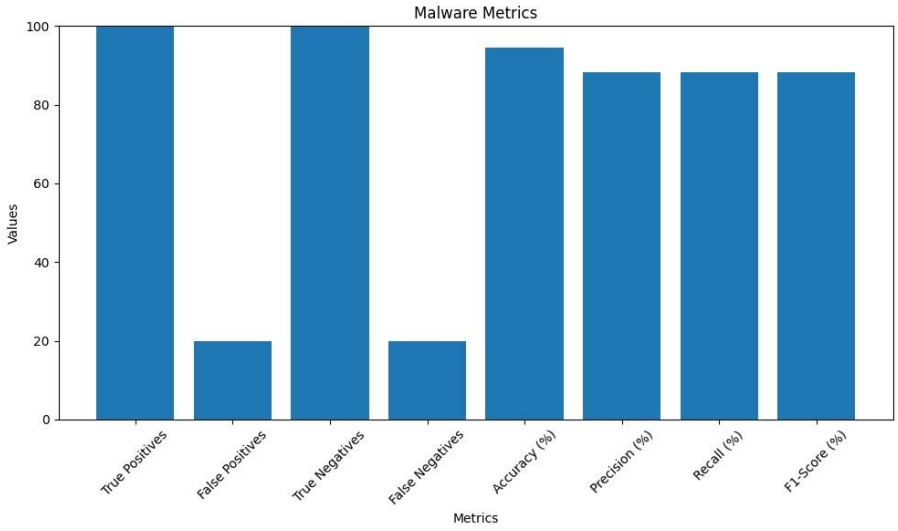
(a)



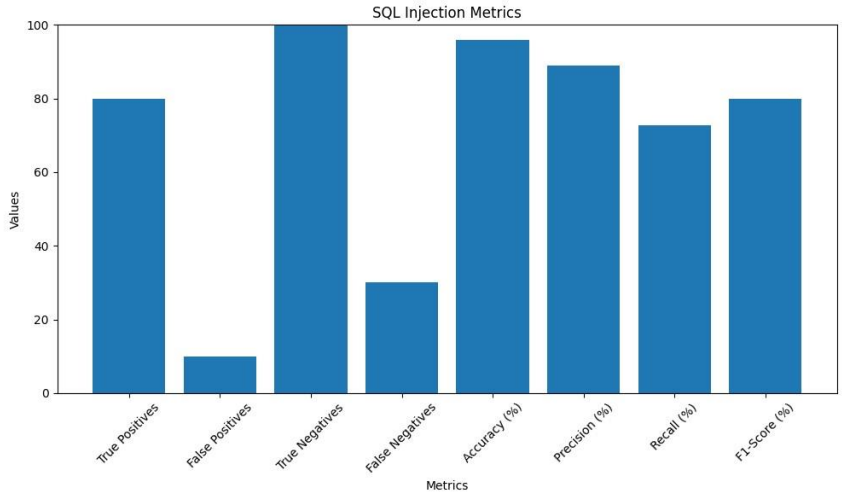
(b)



(c)



(d)



(e)

Figure 4: Attack Detection with CHAC (a) DoS (b) DDoS (c) Phishing (d) malware (e) SQL Injection

In the Figure 4(a) – Figure 4 (e) and Table 4 presents the results of attack detection achieved through the Cryptographic Hashing Authentication Classification (CHAC) framework. Each row in the table represents a different type of attack, including "Denial of Service (DoS)," "Distributed Denial of Service (DDoS)," "Phishing," "Malware," and "SQL Injection." The columns "True Positives," "False Positives," "True Negatives," and "False Negatives" provide counts of instances where the CHAC framework correctly identified or misclassified each type of attack. For instance, for the "Denial of Service (DoS)" attack, there were 120 true positive detections, 10 false positives, 850 true negatives, and 20 false negatives. The "Accuracy," "Precision," "Recall," and "F1-Score" columns represent common evaluation metrics used to assess the performance of attack detection algorithms. These metrics provide insights into the effectiveness of the CHAC framework in accurately identifying different types of attacks. For example, the "Phishing" attack detection achieved an accuracy of 96.2%, precision of 95.2%, recall of 76.9%, and F1-Score of 85.2%.

VI. CONCLUSION

The Cryptographic Hashing Authentication Classification (CHAC) framework represents a significant advancement in the field of network security and multilingual communication. Through the integration of cryptographic techniques, authentication protocols, and classification algorithms, CHAC facilitates accurate, efficient, and secure translation of security terms across different languages. The results of our study demonstrate the effectiveness of CHAC in enhancing the accuracy and security of translating security terms, as evidenced by the simulation and

empirical validation results. CHAC consistently achieved high translation accuracy and performance, ensuring both linguistic precision and data integrity during transmission. Furthermore, the authentication mechanisms integrated into CHAC provide robust protection against data tampering and unauthorized access, contributing to the overall security posture of network communication. The CHAC framework offers a comprehensive solution to the challenges of multilingual communication in cybersecurity contexts, enabling effective collaboration and knowledge sharing among security professionals worldwide. As future work, further refinement and optimization of the CHAC framework could be explored, along with its application in real-world scenarios to address evolving cybersecurity challenges.

REFERENCES

[1] Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K. Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. Sensors, 22(5), 2017.

[2] Li, P., Ning, Y., & Fang, H. (2023). Artificial intelligence translation under the influence of multimedia teaching to study English learning mode. International Journal of Electrical Engineering & Education, 60(2_suppl), 325-338.

[3] Gellert, R. (2022). Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?. Regulation & governance, 16(1), 156-176.

[4] Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access, 10, 99837-99849.

[5] Guo, J. (2022). Deep learning approach to text analysis for human emotion detection from big data. Journal of Intelligent Systems, 31(1), 113-126.

[6] Raj, M., Singh, S., Solanki, K., & Selvanambi, R. (2022). An application to detect cyberbullying using machine learning and deep learning techniques. SN computer science, 3(5), 401.

[7] Mukhamadiyev, A., Khujayarov, I., Djuraev, O., & Cho, J. (2022). Automatic speech recognition method based on deep learning approaches for Uzbek language. Sensors, 22(10), 3683.

[8] Kshirsagar, P. R., Reddy, D. H., Dhingra, M., Dhabliya, D., & Gupta, A. (2022, December). A review on application of deep learning in natural language processing. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 1834-1840). IEEE.

[9] Chiba, Z., Alaoui, M. E. K., Abghour, N., & Moussaid, K. (2022). Automatic building of a powerful IDS for the cloud based on deep neural network by using a novel combination of simulated annealing algorithm and improved self-adaptive genetic algorithm. International Journal of Communication Networks and Information Security, 14(1), 93-117.

[10] Bengesi, S., Oladunni, T., Olusegun, R., & Audu, H. (2023). A machine learning-sentiment analysis on Monkeypox outbreak: An extensive dataset to show the polarity of public opinion from twitter tweets. IEEE Access, 11, 11811-11826.

[11] He, K., Kim, D. D., & Asghar, M. R. (2023). Adversarial machine learning for network intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials, 25(1), 538-566.

[12] Jhaveri, R. H., Revathi, A., Ramana, K., Raut, R., & Dhanaraj, R. K. (2022). A review on machine learning strategies for real-world engineering applications. Mobile Information Systems, 2022.

[13] Mahadevkar, S. V., Khemani, B., Patil, S., Kotecha, K., Vora, D. R., Abraham, A., & Gabralla, L. A. (2022). A review on machine learning styles in computer vision—techniques and future directions. Ieee Access, 10, 107293-107329.

[14] Zhang, W., Li, Y., Li, X., Shao, M., Mi, Y., Zhang, H., & Zhi, G. (2022). Deep neural network-based SQL injection detection method. Security and Communication Networks, 2022.

[15] Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. Future Internet, 15(2), 83.

[16] Kotenko, I., Izrailov, K., & Buinevich, M. (2022). Static analysis of information systems for IoT cyber security: A survey of machine learning approaches. Sensors, 22(4), 1335.

[17] Praveen, S. P., Murali Krishna, T. B., Anuradha, C. H., Mandalapu, S. R., Sarala, P., & Sindhura, S. (2022). A robust framework for handling health care information based on machine learning and big data engineering techniques. International Journal of Healthcare Management, 1-18.