International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Revolutionizing Social Media Security: Integrating Graphic Passwords and Blockchain for Enhanced User Authentication

[1]Geerija Lavania, [2]Dr. Gajanand Sharma

Submitted: 25/12/2023 **Revised**: 29/01/2024 **Accepted**: 10/02/2024

Abstract: The Office of Communications and Marketing oversees various social media platforms, including "Facebook, Twitter, Instagram, LinkedIn, and YouTube." Safeguarding online presence is paramount for any business, emphasizing the crucial role of social media security. Protection measures encompass thwarting targeted phishing attacks, fortifying corporate accounts against hacking, and preventing social engineering scams. Social media platforms like Facebook and Twitter offer opportunities for fraudsters to exploit, employing legitimate but fake accounts to gain trust and extract sensitive information. Scammers adeptly craft fraudulent accounts, mimicking individuals or companies, spreading malware, online attacks, and misinformation to deceive followers and company employees into revealing private data or corporate secrets .To enhance security, an envisioned end-to-end app proposes registering mobile numbers with a password consisting of zigzag images or by sliding computer-generated images to create a unique pattern. This complements the existing module facilitating easier SIM card identification. Decentralized blockchain formed by users in communication, as opposed to a private blockchain with a central authority, is proposed. Our social media platform prioritizes two-factor authentication, requiring users to log in with their email and password, and then verifying the login request with a unique one-time password sent to their phone number during the initiation of the login request.

Keywords: *Social Media Security, User Authentication, Pattern Passwords, Blockchain, User validation, Data Security*

1. Introduction

Social media platforms provide a means for individuals to connect, share, and learn about each other's lives. However, not all sharing is genuine, as many accounts impersonate brands, posing a risk to both business and personal data. Popular platforms like Facebook, Twitter, Google+, and others can be exploited during the reconnaissance phase of social engineering or phishing attacks. Attackers often leverage social media accounts to gather information about targets before launching their attacks [1].

Each social media platform has its unique vulnerabilities. For instance, Facebook enables users to keep images and comments private, prompting attackers to either direct message the target or befriend their friends first [1]. LinkedIn, a networking platform, becomes a target for hackers seeking to exploit its network of colleagues in the same field. An attacker can collect employees' emails for potential phishing campaigns, using publicly available company profiles to target those with access to sensitive information [2].

The impact of information technology on society is evident through the rise of platforms like Facebook, Instagram, WhatsApp, and Line. Changes in culture, ethics, and conventional standards accompany this technological evolution. However, the prevalence of social media also introduces security risks [3]. Cybercriminals may use social media posts to find passwords or impersonate business owners, leading to data breaches and compromises of business infrastructure.

To address these challenges, a proposed research design integrates blockchain technology with advanced AI in social media platforms. The aim is to create transparent, auditable content networks and ranking algorithms that use digital tokens as ranking signals. Novel hybrid algorithms, combining blockchain concepts with AI techniques, will be evaluated for efficacy and performance through numerical simulation results. A qualitative survey on focus groups will further explore public opinions on the intersection of blockchain and social media to restore confidence and combat fake news [4].

The authentication process consists of three phases: registration, login, and verification. During registration, users enter passwords, rate colors during login, and verify the password entered based on the interface shown. Passwords, referred to as secret passes, have a minimum length of 8 characters with an even number of characters. Session passwords are derived from these secret passes. The login process involves a grid-based user interface with alphabets and numbers, varying with each session and distributed randomly on the grid. A comparison table evaluates different authentication

1JECRC University
Girija47lavania@gmail.com
2JECRC University
gajanan.sharma@gmail.com

techniques for social media platforms based on security, cost, usability, and availability of security [4].

2. Literature Review

Shevchuk, R. et al. (2020): The paper explores the awareness of security settings impacting social media users and introduces software designed to automatically assess security settings on social media accounts [1]. The developed software evaluates security settings for Facebook and Instagram, offering recommendations for enhancement.

Huang, S.-Y. and Ban, T. (2020): Organizations are urged not only to maintain up-to-date software but also to effectively manage the latest security updates and address security-related patches[2]. Valuable intelligence on potential threats can be gathered from sources such as computer emergency response teams, cybersecurity news, the national vulnerability database, or commercial cybersecurity vendors. Social media is identified as another potential intelligence source. This project utilizes publicly accessible internet resources to predict the exploitation likelihood of vulnerabilities in specific computer applications, considering various factors, including contextual information, machine learning techniques for Twitter, and AI-enabled modules integrated into a threat intelligence platform.

Ekwunife, N. (2020): Social media is recognized as the most responsive internet communication method, shaping interpersonal communication, opinion sharing, and real-time interaction for diverse user groups. The study proposes a machine learning model to enhance quick intervention actions by mining social media data, aiming to establish automated systems for intelligence agencies to prevent national events [3].

Guidi, B. and Michienzi, A. (2020): While some view OSNs like Instagram and Whatsapp as effective communication and content-sharing platforms, privacy concerns arise due to potential exploitation in decentralized solutions like blockchain. The paper argues for insights from social networks to create detection features for bot usage and explores Steemit as a popular type of BOSM, revealing that bots are more active than human users [4].

Lai, J. (2019): The paper examines cross-border e-commerce logistics supply chain management, proposing innovative applications of blockchain's decentralization in logistics, capital flow, and information flow. It presents new ideas for building an efficient cross-border e-commerce logistics supply chain system, enhancing China's capability in managing such chains, and addressing development challenges under the One Belt And One Road strategy [5].

Shevchuk, R. and Pastukh, Y. (2019): The paper focuses on improving the security level of social media accounts and developing a mathematical model for measurement. A chatbot is introduced to provide recommendations for enhancing an account's security level as needed [6].

Table 1. Findings in Literature Review

Author Name	Year	Main Concepts	Objectives
Shevchuk, R. et al.	2020	Social media security settings, software	Investigate and increase awareness of social media security settings. Develop software for automated assessment and provide improvement recommendations [1].
Huang, S.-Y. and Ban, T.	2020	Cybersecurity, social media intelligence, machine learning	Explore diverse sources for cybersecurity intelligence, forecast vulnerability exploitation, and implement AI-enabled modules for enhanced threat intelligence [2].
Ekwunife, N.	2020	Social media communication, machine learning	Propose a machine learning model to improve rapid intervention through the mining of social media data for national security purposes [3].
Guidi, B. and Michienzi, A.	2020	OSNs, privacy concerns, blockchain, bot detection	Examine privacy challenges in online social networks, advocate for insights from these networks, and investigate Steemit for the detection of bots [4].
Lai, J.	2019	Cross-border e-commerce logistics, blockchain	Explore applications of blockchain in logistics, capital flow, and information flow to enhance the efficiency of cross-border e-commerce [5].
Shevchuk, R. and Pastukh, Y.	2019	Social media account security, mathematical model	Enhance the security of social media accounts and develop a mathematical model for measurement. Introduce a chatbot to provide security

recommendations [6].

3. Materials and Methods

Materials and Methods for Investigating Graphic Passwords and Blockchain Security in Social Media Platforms:

3.1. Materials:

- Digital Devices: Utilize a diverse range of digital devices, including smartphones, tablets, and computers, to assess the compatibility of the envisioned graphic password system.
- Graphical Passwords: Design and deploy a collection of graphical passwords, comprising images and image-based patterns. Curate a varied selection of images to ensure the efficacy and security of the graphical password authentication method [21][7].
- Tokens: Employ tokens as concealed keys for token-based authentication. Explore various token designs and images to enhance security.
- Blockchain Technology: Implement blockchain technology to fortify social media platforms. Establish a blockchain network for validating user authentication and securing message exchanges[22][8].
- Zig-Zag Arrangement: Develop and implement the Zig-Zag arrangement for authentication in social media platforms [9].

3.2. Methods:

- Graphic Password Authentication: Conduct user studies to assess the memorability and security of graphical passwords. Analyze the effectiveness of image-based passwords against dictionary attacks, keyloggers, and social engineering [10].
- Token-Based Authentication: Evaluate the use of tokens as concealed keys for authentication. Assess the ease of use and security benefits of token-based authentication.
- Blockchain Integration: Implement blockchain technology for user authentication in social media platforms. Analyze the impact of blockchain on information security, privacy, and public sector confidence.
- Zig-Zag Arrangement for Social Media Security: Develop and implement the Zig-Zag arrangement for authentication in social media platforms. Evaluate the security enhancements provided by the Zig-Zag arrangement in protecting user information.
- Data Access Point Authentication: Investigate and implement data access point authentication for customer security assurance. Assess the efficacy of data access point authentication in specific scenarios [11].
- Comparative Analysis: Perform a comparative analysis between traditional authentication methods and the proposed graphic password, token-based authentication, blockchain integration, and Zig-Zag arrangement for social media security.
- Numerical Simulation: Conduct numerical simulations to evaluate the efficacy and performance of the proposed security model on social media platforms.
- Ethical Considerations: Ensure adherence to ethical standards in research involving user data and privacy [12].

These materials and methods seek to comprehensively investigate and validate the proposed security model, incorporating graphic passwords, token-based authentication, blockchain technology, Zig-Zag arrangement, and data access point authentication for enhanced security in social media platforms..

3.3 Algorithms

Algorithm: UserAuthentication

Input:

- Username
- Password
- Mobile Number
- IMEI Number

Output:

- User authentication status

Procedure:

1. Read user credentials (Username, Password).
2. Set matrix dimension (matrix Dimension).
3. Generate a random image matrix (imageMatrix) with the dimension matrixDimension.
4. Read Mobile Number and IMEI Number.
5. Process Mobile Number using the SHA-512 hash algorithm and store the hash in mobHash.
6. Extract the last two digits of the IMEI number and store it in extractionValue.
7. Prompt the user to draw a Zig-Zag pattern over the matrix and generate the pattern of the images using the selected images in the Zig-Zag pattern (zig-ZagPattern).

8. Generate the SHA-512 hash of the images selected in the Zig-Zag pattern and extract N characters from each image hash. Store the result in imgHash.

9. Set up a blockchain for user identity using N characters extracted from mobHash + IMEI Number + imgHash.

10. Store all details (Username, Password, Mobile Number, IMEI Number, Blockchain Data) in the database.

11. Return the user authentication status.

End Algorithm

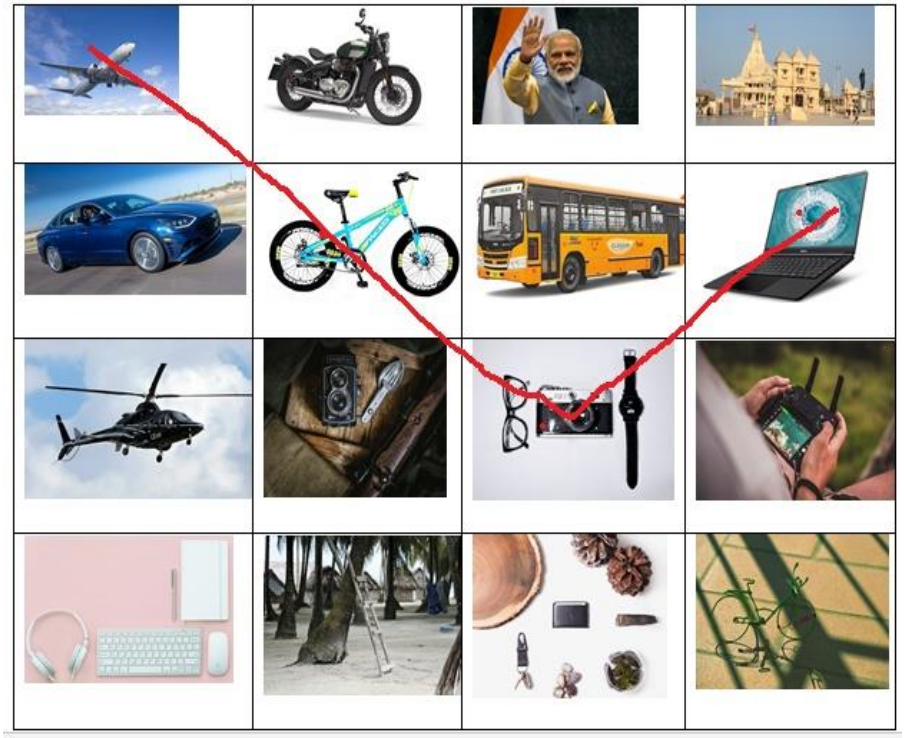

Fig 1. Zig Zag Pattern of Images

The "User Authentication" algorithm is a comprehensive authentication mechanism that incorporates traditional and innovative security measures to enhance the overall robustness of user identity verification. Beginning with the retrieval of standard user credentials, such as the username and password, the algorithm introduces a matrix of random images and prompts users to draw a Zig-Zag pattern over it, adding a graphical and interactive layer to the authentication process. The algorithm employs cryptographic techniques, including the SHA-512 hash algorithm, to process the user's mobile number and extract relevant information from the IMEI number. The resulting data, along with the graphical pattern and hashed images, are securely integrated into a blockchain, establishing a tamper-resistant record of user identity. The algorithm concludes by storing all pertinent details, including username, password, mobile number, and blockchain data, in a secure database. Through its multi-faceted approach, the algorithm aims to provide heightened security for user authentication in social media platforms, offering protection against common threats such as password-related attacks and unauthorized access.

Algorithm: Secure Message Communication

Input:

- Sender
- Receiver
- Message

Output:

- Status of message communication

Procedure:

1. Choose the sender.

2. Prepare the message.

3. When the user sends the message, the underlying blockchain generation includes the following: a. Authenticate the sender's pattern and store it in SENDPATTERN. b. Authenticate the receiver's pattern and store it in RECPATTERN. c. Generate SHA-512 extract for the sent message and store it in MSGHASH. d. Create a combination of Date Time Stamp + Message Unique Serial Number Pattern + Secure Pin. e. Merge patterns from steps a and b with MSGHASH, Date Time Stamp, and Secure Pin to create a new blockchain.

4. Save the details in the database.

5. End the algorithm.

The Secure Message Communication algorithm is designed to ensure a secure and authenticated exchange of messages between a designated sender and receiver. It initiates by selecting the sender and preparing the intended message for transmission. As the user sends the message, a series of background processes unfold. Firstly, the algorithm authenticates and stores the sender's pattern as SENDPATTERN, followed by a similar authentication process for the receiver's pattern, stored as RECPATTERN. Further, a SHA-512 extract is generated for the sent message and stored as MSGHASH. To enhance security, the algorithm creates a unique combination involving the Date Time Stamp, Message Unique Serial Number Pattern, and a Secure Pin [13]. These components, along with the authenticated patterns from both sender and receiver, are amalgamated to form a new blockchain, ensuring the integrity of the communication process. The algorithm concludes by storing relevant details in the database, marking the completion of a comprehensive and secure message exchange protocol [14]. The practical application involves coding these sequential steps in a programming language, incorporating functions for hash generation, pattern authentication, and database interactions, among other crucial elements [15].

4. Results

Contains the sample number

9828041224

IMEI 1:

864363032757384

Photo 1

69fa972f6066e2667a32c648333aa923f651454893519cb
c370fdfc035a7e476e1128e718d02f7a4d5f2cb1cf5d1b6e
6ab7188212bf8a3a288f2e271ac825b8b

Photo 2

39067f315f86a11550052de5530d4edd7ab7730e176d968
708e5923bd0f7bba27d86603f7a11b0304654e51f85d36d
9eab0303dbabb5d3eb0851b124650871c4

Photo 3

e5abd4da9c07a89a6db88e3d30f18a4ccbbeaf6e74e46d1a
11a7665c8defd26e9bb8325975c86b0abbcf9974111fc8f8
5bd6bbf982de3229b3043dff2f83b549

Photo 4

b089e5d1e5309179da095fe7c5958110f3339f1b9ddcb29
47ab9ab928cc144ce19ee42e19663534673de31320d29c2
dd42759b48788a4b4540d1f0ca21716976

N=24 (last 2 digits of mobile number)

Final Blockchain

cfd41541c17b42ae2b9b075+"-
"+864363032757384+69fa972f6066e2667a32c64+"-
"+39067f315f86a11550052de+"-
"+e5abd4da9c07a89a6db88e3+"-
"+b089e5d1e5309179da095fe

Entropy Examination

Understanding password strength and security is fundamental, with password entropy serving as a key concept in this regard. Password entropy measures the level of unpredictability or randomness within a password, indicating the difficulty an attacker would face in guessing or cracking it through brute-force methods. The primary influencers of password entropy are the character set size (number of possible characters) and the length of the password. A larger character set and increased password length result in higher entropy, elevating the strength and security of the password. The formula for calculating password entropy is expressed as Entropy = log2(N^L), where N represents the character set size, L is the password length in characters, and log2 signifies the logarithm base 2. The resulting measurement is typically in bits. To ensure the creation of robust and secure passwords, it is imperative to utilize a diverse character set and opt for longer passwords. Passphrases, composed of sequences of words or sentences, provide a means to significantly boost password entropy while remaining memorable. Additionally, combining strong passwords with multi-factor authentication (MFA) introduces an extra layer of protection, augmenting overall security [16].

Table 2. Entropy Examination using Years to Broke

Tool Name	Result
Security.org Tool	“3 hundred quadrillion octogintillion years”
Password Monster Tool	“10 trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion years”
Delinea Tool	“1,290,327,861,965,751,700 octogintillion years”

The entropy results show how much time in years is required to break the blockchain, and thus the blockchain formed is strong.

4. Discussion

The proposed research is centred on elevating the security standards of user authentication and message communication within social media platforms through the implementation of innovative techniques such as graphic passwords, blockchain integration, and the Zig-Zag arrangement. The discourse emphasizes the significance and potential ramifications of these methods in confronting contemporary challenges related to cybersecurity and privacy within the social media landscape [17].

A pivotal aspect of the research involves the introduction of graphic passwords, capitalizing on the human brain's ease of memorizing images. The utilization of random images and the Zig-Zag arrangement is intended to offer a secure and user-friendly authentication approach. By leveraging SHA-512 hash algorithms and incorporating mobile numbers and IMEI numbers, the research seeks to strengthen the authentication process, rendering it resistant to various cyber threats like phishing and social engineering.

The incorporation of blockchain technology into social media platforms is a noteworthy proposition in the research. The decentralized and secure nature of blockchain is anticipated to enhance information security and privacy. The discourse explores how the suggested hybrid algorithms, merging blockchain concepts and AI techniques, could establish transparent and auditable content networks, potentially mitigating issues related to fake news and restoring public confidence[18][19]. The research also delves into securing message communication through blockchain, employing sender and receiver authentication patterns. By establishing a new blockchain for each communication process, and integrating timestamps and unique serial numbers, the research addresses the challenge of ensuring the confidentiality and integrity of exchanged messages [20].

The Zig-Zag arrangement for usage authentication and the innovative theoretical framework for integrating blockchain technology into social platforms represent novel contributions. The discourse underscores the potential benefits of these approaches in thwarting cyber threats, diminishing the risk of data breaches, and fostering a more secure and trustworthy social media environment.

Furthermore, the proposed research emphasizes the importance of two-factor authentication in social media platforms, encompassing both email and phone number verification. This dual-layered security approach adds an extra barrier against unauthorized access and potential data breaches.

In conclusion, the discourse underscores the significance of the proposed research in advancing the field of social media security. The integration of graphic passwords, blockchain technology, and the Zig-Zag arrangement provides a multifaceted strategy to tackle the evolving challenges of cybersecurity, privacy concerns, and the proliferation of online threats within social media platforms. The research establishes a foundation for more robust and resilient security measures, contributing to a safer and more trustworthy online social experience.

5. Conclusions

In conclusion, this research endeavors to significantly elevate the security infrastructure of social media platforms through a comprehensive approach encompassing graphic passwords, blockchain integration, and the innovative Zig-Zag arrangement. By tackling crucial aspects of user authentication and message communication, the study aims to address contemporary challenges related to cybersecurity, privacy, and the growing prevalence of online threats.The introduction of graphic passwords, crafted with random images and the Zig-Zag arrangement, introduces a user-friendly yet robust authentication method. Capitalizing on the human brain's ability to memorize images, this approach adds an additional layer of security to safeguard user credentials. The integration of SHA-512 hash algorithms, alongside mobile numbers and IMEI numbers, contributes to a more resilient defense against phishing attacks, social engineering, and other cybersecurity threats.The incorporation of blockchain technology into social media platforms represents a groundbreaking initiative. The proposed hybrid algorithms, merging blockchain concepts with advanced AI techniques, aim to establish transparent and auditable content networks. This approach holds promise in combating the spread of fake news, ensuring information security, and restoring public confidence in social media.The research extends its focus to secure message communication, introducing a novel blockchain generation process. By authenticating sender and receiver patterns, generating SHA-512 extracts for messages, and incorporating unique serial numbers and timestamps, the study strives to fortify the confidentiality and integrity of exchanged messages.

Furthermore, the Zig-Zag arrangement for usage authentication and the theoretical framework for blockchain integration offer novel contributions to the field. These innovative methods, combined with the implementation of two-factor authentication using email and phone number verification, collectively strengthen the security posture of social media platforms.

In essence, this research lays the foundation for a more secure and trustworthy social media environment. By amalgamating cutting-edge technologies and novel methodologies, the study addresses critical security gaps, reduces the risk of data breaches, and enhances user confidence in online interactions. The proposed measures not only bolster the protection of sensitive user information but also contribute to the ongoing discourse on fortifying digital landscapes against the ever-evolving landscape of cyber threats. As social media platforms continue to play an integral role in global communication, the insights derived from this research have the potential to shape the future of online security and foster a safer digital experience for users worldwide.

References

[1] Shevchuk, R., Melnyk, A., Opalko, O., & Shevchuk, H. (2020). Software for automatic estimating security settings of social media accounts. In 10th International Conference on Advanced Computer Information Technologies (ACIT), 2020.

[2] Huang, S.-Y., & Ban, T. (2020). Monitoring social media for vulnerability-threat prediction and topic analysis. In IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020.

[3] Ekwunife, N. (2020). National security intelligence through social network data mining. In IEEE International Conference on Big Data (Big Data), 2020.

[4] Guidi, B., & Michienzi, A. (2020). Users and Bots Behavior Analysis in Blockchain Social Media. In Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS), 2020.

[5] Lai, J. (2019). Research on cross-border E-commerce logistics supply under the blockchain. In International Conference on Computer Network, Electronic and Automation (ICCNEA), 2019.

[6] Shevchuk, R., & Pastukh, Y. (2019). Improve the security of social media accounts. In 9th International Conference on Advanced Computer Information Technologies (ACIT), 2019.

[7] Shree, J., Kanimozhi, N. R., Dhanush, G. A., Haridas, A., Sravani, A., & Kumar, P. (2020). To Design a Smart and Secure Purchasing System integrated with ERP using Blockchain technology. In IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 2020.

[8] Soumya, T. R., & Revathy, S. (2018). Survey on threats in online social media. In International Conference on Communication and Signal Processing (ICCSP), 2018.

[9] Teja, J. R. (2020). Proposing a method for Public record maintenance using Blockchain. In International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020.

[10] Tse, D., Huang, K., Cai, B., & Liang, K. (2018). Robust password-keeping system using block-chain technology. In IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2018.

[11] Wang, Z., et al. (2015). Key technology research on user identity resolution across multi-social media. In International Conference on Cloud Computing and Big Data (CCBD), 2015.

[12] Chattopadhyay, A., Christian, D., Ulman, A., & Sawyer, C. (2018). A middle-school case study: Piloting a novel visual privacy themed module for teaching societal and human security topics using social media apps. In IEEE Frontiers in Education Conference (FIE), 2018.

[13] Chung, W., Mustaine, E., & Zeng, D. (2017). Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking. In IEEE International Conference on Intelligence and Security Informatics (ISI), 2017.

[14] Colbaugh, R., & Glass, K. (2013). Analyzing social media content for security informatics. In European Intelligence and Security Informatics Conference, 2013.

[15] Cui, Z., et al. (2020). A hybrid BlockChain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing.

[16] Garcia, C., Rabadi, G., Abujaber, D., & Seck, M. (2023). Supporting humanitarian crisis decision-making with reliable intelligence derived from social media using AI. Journal of Homeland Security and Emergency Management, 0(0).

[17] Kurniawan, E., & Riadi, I. (2018). Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-CMM. [Journal Name], 16(1), 139–147.

[18] Riadi, I., Aristianto, E. I., & Dahlan, A. (2016). An Analysis of Vulnerability Web Against Attack Unrestricted Image File Upload. Computer Engineering and Applications, 5(1), 19–28.

[19] Angga, C. (2011). Analysis of How Diverse Works Hash Functions Exist, 1–6.

[20] Jing, T. W., & Murugesan, R. K. (2019). A Theoretical Framework to Build Trust and Prevent Fake News in Social Media Using Blockchain. In IRICT 2018, AISC 843, 955–962. Springer Nature Switzerland AG 2019 F. Saeed et al. (Eds.).

[21] Lavania, G.,& Sharma, G. (2022, December). Blockchain and its dimensions: Future Security. In Proceedings of the 4th International Conference on Information Management & Machine Intelligence (pp. 1-4).

[22] Lavania, G., & Sharma, G. (2021, September). Security on Social Media Platform Using Private Blockchain. In International Conference on Cyber Security, Privacy and Networking (pp. 217-226). Cham: Springer International Publishing.

[23] Goyal, D., Lavania, G., & Sharma, G. (2023, June). Review of modern web application cyber security risks and countermeasures. In AIP Conference Proceedings (Vol. 2782, No. 1). AIP Publishing.