BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **23**, No 3
Sofia • 2023 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2023-0027

User Behavior Analysis for Detecting Compromised User Accounts: A Review Paper

M. Jurišić, I. Tomičić, P. Grd

Faculty of Organization and Informatics, University of Zagreb, Varazdin, Croatia
E-mails: marko.jurisic@foi.unizg.hr igor.tomicic@foi.unizg.hr petra.grd@foi.unizg.hr

***Abstract*:** *The rise of online transactions has led to a corresponding increase in online criminal activities. Account takeover attacks, in particular, are challenging to detect, and novel approaches utilize machine learning to identify compromised accounts. This paper aims to conduct a literature review on account takeover detection and user behavior analysis within the cybersecurity domain. By exploring these areas, the goal is to combat account takeovers and other fraudulent attempts effectively.*

***Keywords*:** *Machine learning, account takeover, ATO, user behavior analysis, literature review.*

1. Introduction

The surge in online transactions has also led to a rise in various fraud attempts, and their number has increased even more during the COVID-19 pandemic [1]. Account takeover is especially hard to detect because the compromised accounts can be dormant for a long time, or intruder activity can be interspersed with regular users' activities [2]. One effective approach to combat fraud is to apply user behavior analytics and profiling. By analyzing user behavior patterns and establishing user profiles, it becomes possible to identify potential anomalies, flag suspicious user accounts, and take other appropriate actions to mitigate risks. One of the challenges in conducting research in the field of account takeover and user behavior analysis is the lack of published datasets containing real data. This limitation makes it difficult to evaluate and compare different methods accurately. Additionally, another hurdle is the inconsistency in the methods and metrics used across various papers that apply machine-learning techniques.

To address these issues, this paper aims to provide an overview of the methods and metrics employed in the research areas of account takeover and user behavior analysis. By synthesizing and analyzing existing literature, it seeks to establish a comprehensive understanding of the current approaches and evaluation measures used in this domain.

2. Related work

Limited research has been conducted on account takeover specifically in the context of online marketplaces. However, there is a notable paper by the mobile.de team that concentrates on the institutional seller account takeover. This paper presents a case study where machine learning techniques were employed to prevent such account takeovers [2]. Additionally, another paper explores different algorithms using H2O and Catboost open-source libraries [3].

User behavior analysis encompasses diverse fields like telecommunication and marketing, but this research specifically concentrates on user behavior analysis within the context of cybersecurity and account takeover. By narrowing the focus to this specific domain, the study aims to delve into the intricacies and challenges associated with analyzing user behavior patterns to detect and prevent account takeover incidents.

3. Methodology

The purpose of the literature review is to summarize the existing research and to provide a background in order to position further research activities [4]. The review process typically consists of three main phases: planning the review, conducting the review, and reporting the review.

3.1. Research questions

The most important part of a literature review is specifying the research questions [4]. The goal of this paper is to give an overview of previous work in the areas of:

- Account TakeOver (ATO).
- User Behavior Analysis (UBA), in the context of security/fraud detection.
- Datasets suitable for training machine learning models for UBA/ATO.

Research questions are defined as following:

- Which datasets are used for research in UBA and ATO?
- Which methods are used for research in UBA and ATO?
- Which metrics are used for research in UBA and ATO?

3.2. Search strategy

For this research, the Scopus and Web of Science databases have been utilized, as they are widely recognized and commonly used in academic research to access a broad range of scholarly articles across various disciplines. Queries have been adjusted so that they include both British and American spelling variants. The initial results are shown in Table 1. The search was done on the 26th of January 2023.

Table 1. Queries and initial results

Query	Results WoS	Results scopus
(”hacked account∗” OR ”compromised account∗” OR ”hijacked account∗” OR ”breached account∗” OR ”stolen account∗” OR ”account∗ takeover∗”) AND (”machine learning” OR ”deep learning” OR ”artificial intelligence” OR ” hidden markov models ” OR ai OR ml OR lstm OR hmm OR ncde)	29	40
(”user behavior analysis” OR ”user behavior analytics” OR ”user behavior analysis ” OR ”user behavior analytics”) AND (” fraud detection ” OR security OR cybersecurity)	69	134

3.3. Study selection

Inclusion criteria:

- Computer science research area.
- Keywords contained in title, abstract, or keywords (in any variant).
- Papers focusing on recognizing compromised accounts (not prevention).

Exclusion criteria:

- Papers not in English.
- Papers not published in journals or conference proceedings (no peer review).
- Papers not discussing machine learning or statistical methods.

Initially, the ATO search produced 69 results and UBA search produced 203 results. After removing duplicates, there were 46 papers left for ATO and 142 for UBA. After applying initial inclusion and exclusion criteria, 30 papers have been left for ATO and 64 for UBA to review in detail. Some papers were not available through National and University Library proxy and had to be left out of the research.

After reading the full text of available papers and including papers from review articles [5, 6] that have been not covered using original queries, 23 papers for ATO and 49 for UBA were included in the final research body.

4. Results and discussion

This chapter presents the data synthesis answers to research questions in form of text, figures and tables. Figs 1 and 2 show that the research interest in ATO and UBA in the cybersecurity continuously grows.

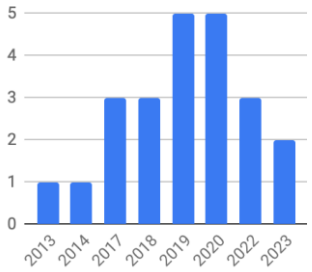

Fig. 1. ATO papers by year

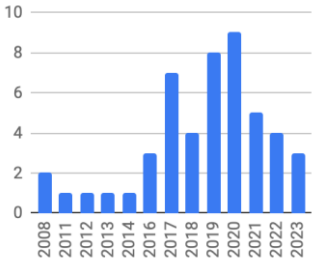

Fig. 2. UBA papers by year

4.1. Which datasets are used for research in UBA and ATO?

Most authors use private datasets, and there is a lot of usage of Twitter data for ATO [7-12], possibly because the Twitter API was freely available and allowed for relatively straightforward data collection and filtering processes. The accessibility and simplicity of the Twitter API made it a convenient source of data for researchers exploring ATO-related topics. There are also some approaches to scraping the data from Amazon [13], Facebook [14], and Google+ [10]. For UBA, the CERT dataset appears to be the most utilized [15-19], and [79]. This dataset's popularity can be attributed to its comprehensiveness, as it includes various types of attacks and is more recent compared to other available datasets. Researchers often choose the CERT dataset as it provides a diverse range of attack scenarios, enabling them to analyze user behavior and develop effective detection mechanisms in UBA research. Comparison can be seen in Figs 3 and 4. LANL dataset is referenced by two papers [22, 78]. There is one paper each referencing the SEA dataset [20], KDD dataset [21], and Azure Public dataset [23].

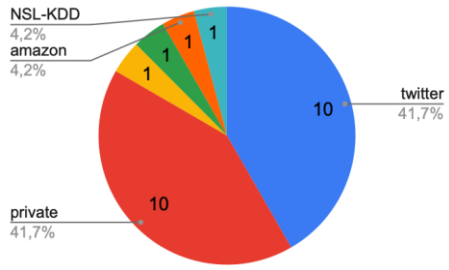

Fig. 3. ATO datasets

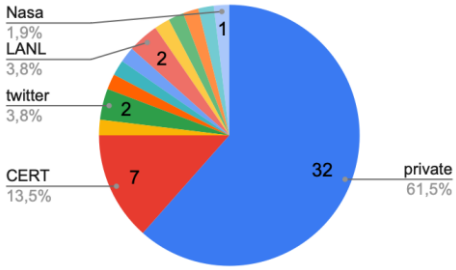

Fig. 4. UBA datasets

4.2. Which methods are used for research in UBA and ATO?

Methods are a bit harder to extract than datasets, since many authors extend existing methods (like [24] with Hidden Markov model extensions, or [25] with LSTM graph extensions, [10, 26] extend autoencoders approach), or use alternative names, e.g. J48 in Weka machine learning kit [8, 27] which is an implementation of C4.5 [28] or, generally said, a decision tree [29, 30].

Still, there are general approaches that are used very often such as bagging [31], boosting, [32, 33], and rule engines [34-36]. Random Forests (RF) are one of the most widely used methods, either because they are an established method and included in various machine learning tools [8, 27], used as a benchmark [2], or used in an ensemble together with other methods such as in [37]. Clustering variants are also used: k-means [38, 39, 29, 40, 41], dbscan [23], c-means [42]. Support Vector Machines (SVM) are also used, sometimes as a single [43] or best classifier in the experiment [29, 44] and sometimes to support a claim that another method performs better [45]. Bayesian approaches (Naive Bayes [46, 47] Naive Bernoulli Bayes [2], Bayes net [8, 48, 42]) are also used very often, with the argument that they are simple and fast to train and still have a surprisingly good performance.

From neural network approaches [49], Long Short-Term Memory networks (LSTM) [19, 50] and variants [51] are used very often, because they model temporal data very well, and autoencoder variants [52, 51] are often used for anomaly detection. One of the latest developments is the use of a sequential hierarchical memory (s.SCASHM) model [53], which gives very promising results.

One assumption might be that more traditional methods such as RF would not be used in the most recent literature since neural network approaches are getting more and more prevalent, but there are older papers using neural networks [54] and recent papers exclusively using Petri nets [55] and hidden Markov models [56, 24, 57].

Table 2. A summary table

Method class	Papers
Decision trees	[8], [27], [58], [28], [29], [30], [48], [41], [75]
Bayesian	[8], [46], [27], [58], [2], [28], [29], [47], [48], [41], [42], [31], [76], [77]
RNN	[12], [25], [51], [59], [19], [50], [18], [45], [78]
Markovian	[24], [57], [56]

4.3. Which metrics are used for research in UBA and ATO?

Most of the papers focus on one method and usually compare it with other methods, arguing as to why the proposed method is better than the ones previously used. Most authors use multiple metrics sourced from the confusion matrix, with a combination of accuracy, recall, precision, and F1 score being the most prominent [7, 8, 46, 60-63]. Many authors also use the Receiver Operating Characteristics (ROC) curve [37, 27, 78] for visualization and the Area Under the ROC curve (AUC) as a scalar value for simpler model performance comparison [25, 64, 10, 65, 66]. Some authors also emphasize that accuracy alone is not enough, due to imbalanced datasets, but some still use only accuracy [58, 67, 59, 36]. A few authors also use other metrics in combination with the aforementioned, such as specificity [68, 24], true/false detection rate [69], the rate of true positives [54] or negatives, or the number of false alarms [21, 20], since false alarms can pose significant cost [31] if one has to check them manually. Mean average error [48], mean average precision [70] error rate [71], and similar metrics are used rarely, since ATO and UBA in the context of cybersecurity are, in their essence, classification problems.

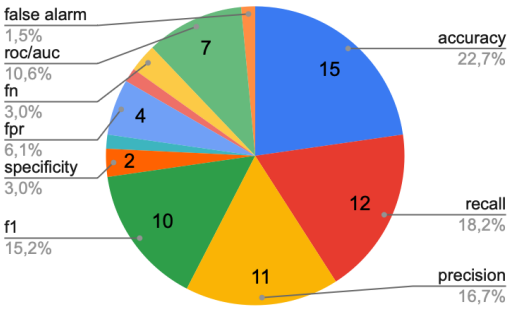

Fig. 5. ATO metrics

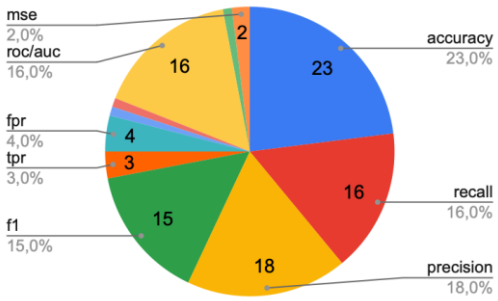

Fig. 6. UBA metrics

5. Limitations and future work

A few papers could not be accessed due to subscription limitations. The authors have been contacted directly but the papers were not received until the closing date for the article and thus could not be included in the research. Therefore, this literature review cannot be considered as a complete state of research in the ATO and UBA areas.

The next step would be to broaden the search to include all papers referencing the CERT dataset. Since it has been extensively used in the referenced papers, this approach would provide new insights into the directions of research in intrusion detection and machine learning.

5. Conclusion

Most authors use different metrics and datasets when testing new approaches in machine learning, which makes it hard to compare them. Interesting to note is that there is no substantial difference observed between the methods and metrics used for Account TakeOver (ATO) and User Behavior Analysis (UBA). This similarity could be attributed to the shared focus on machine learning and security in both research domains. Despite the specific contexts of ATO and UBA, the utilization of similar approaches and metrics suggests commonalities in the underlying techniques employed to address security challenges in these areas.

No dataset was found that would focus on account takeover; most authors either use private datasets, scrape social media platforms for content or use CERT insider threat dataset.

The literature review does not reveal a clear and distinct direction of research in the field. It has been observed that classical methods such as Random Forests (RF), Naive Bayes (NB), and Hidden Markov Models (HMM) are still commonly used, even in 2023 [75-77]. However, there are also promising emerging approaches such as Long Short-Term Memory (LSTM) and autoencoders that have gained attention. These newer methods hold potential for advancing intrusion detection and machine learning in the context of security. Approaches from different contexts could be further analyzed, such as in [72], where authors are arguing on defending against identity threats using risk-based authentication to make identity security adaptive and risk-based. In a related domain tackling Intrusion Detection Systems (IDS), authors propose a hybrid feature selection for the IDS network, based on an ensemble filter, and an improved Intelligent Water Drop (IWD) wrapper [73]. Another aspect worth looking into is the malware; some of the approaches to control, prevention, and protection of computer networks from malware intrusions include mathematical modeling, such as [74], where “the behavior of the computer network under a malware attack is described by a system of nonhomogeneous differential equations”.

The presence of both classical and innovative techniques suggests a diverse landscape of research approaches, indicating ongoing exploration and experimentation in the field.

References

1. Kemp, S., D. Buil-Gil, A. Moneva, F. Miro-Llinares, N. Díaz-Castano. Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. – Journal of Contemporary Criminal Justice, Vol. **37**, 2021, No 4, pp. 480-501.
2. Kawase, R., F. Diana, M. Czeladka, M. Schuler, M. Faust. Internet Fraud: The Case of Account Takeover in Online Marketplace. – In: Proc. of 30th ACM Conference on Hypertext and Social Media, 2019, pp. 181-190.
3. Dekou, R., S. Savo, S. Kufeld, D. Francesca, R. Kawase. Machine Learning Methods for Detecting Fraud in Online Marketplaces. – In: Proc. of CIKM Workshops, 2021.
4. Keele , S., et al. Guidelines for Performing Systematic Literature Reviews in Software Engineering. 2007.
5. Martın, G. A., A. Fernandez-Isabel, I. Martın de Diego, M. Beltran. A Survey for User Behavior Analysis Based on Machine Learning Techniques: Current Models and Applications. – In Applied Intelligence, Vol. **51**, 2021, No 8, pp. 6029-6055.
6. Xin, Y., C. Zhao, H. Zhu, M. Gao. A Survey of Malicious Accounts Detection in Large-Scale Online Social Networks. – In: Proc. of 4th IEEE International Conference on Big Data Security on Cloud, Big Data Security, 2018, pp. 155-158.
7. Zangerle, E., G. Specht. "Sorry, I Was Hacked" a Classification of Compromised Twitter Accounts. – In: Proc. of ACM Symposium on Applied Computing, 2014, pp. 587-593.
8. Singh, M., D. Bansal, S. Sofat. Who is Who on Twitter-Spammer, Fake or Compromised Account? A Tool to Reveal True Identity in Real-Time. – Cybernetics and Systems, Vol. **49**, 2018, No 1, pp. 1-25.
9. Kaur, R., S. Singh, H. Kumar. TB-CoAuth: Text Based Continuous Authentication for Detecting Compromised Accounts in Social Networks. – Applied Soft Computing Journal, Vol. **97**, 2020.
10. Boahen, E., B. Bouya-Moko, F. Qamar, C. Wang. A Deep Learning Approach to Online Social Network Account Compromisation. – In: IEEE Transactions on Computational Social Systems, 2022, pp. 1-13.
11. VanDam, C., F. Masrour, P.-N. Tan, T. Wilson. You Have Been Caute! Early Detection of Compromised Accounts on Social Media. – In: Proc. of 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2019, pp. 25-32.
12. Karimi, H., C. Vandam, L. Ye, J. Tang. End-to-End Compromised Account Detection. – In: Proc. of 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM, 2018, pp. 314-321.
13. Hooi, B., K. Shin, H. A. Song, A. Beutel, N. Shah, C. Faloutsos. Graph-Based Fraud Detection in the Face of Camouflage. – ACM Transactions on Knowledge Discovery from Data (TKDD), Vol. **11**, 2017, No 4, pp. 1-26.
14. Egele, M., G. Stringhini, C. Kruegel, G. Vigna. Towards Detecting Compromised Accounts on Social Networks. – IEEE Transactions on Dependable and Secure Computing, Vol. **14**, 2015, No 4, pp. 447-460.
15. Singh, M., B. Mehtre, S. Sangeetha. Insider Threat Detection Based on User Behaviour Analysis. – In: Communications in Computer and Information Science. Vol. **1241**. 2020, CCIS, pp. 559-574.
16. Glasser, J., B. Lindauer. Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data. – In: Proc. of 2013 IEEE Security and Privacy Workshops, 2013, pp. 98-104. DOI:10.1109/SPW.2013.37.
17. Singh, M., B. Mehtre, S. Sangeetha. User Behavior Based Insider Threat Detection Using a Multi Fuzzy Classifier. – Multimedia Tools and Applications, Vol. **81**, 2022, No 16, pp. 22953-22983.
18. Singh, M., B. Mehtre, S. Sangeetha. User Behaviour Based Insider Threat Detection in Critical Infrastructures.– In: Proc. of International Conference on Secure Cyber Computing and Communications (ICSCCC'2021), 2021, pp. 489-494.

19. A l s h e h r i, A., N. K h a n, A. A l o w a y r, M. A l g h a m d i. Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. – Computer Systems Science and Engineering, Vol. **44**, 2023, No 2, pp. 1679-1689.
20. W u, H.-C., S.-H. H u a n g. User Behavior Analysis in Masquerade Detection Using Principal Component Analysis. – In: Proc. of 8th International Conference on Intelligent Systems Design and Applications, ISDA 2008, Vol. **1**, pp. 201-206.
21. B o a h e n, E., W. C h a n g d a, B.-M. B r u n e l E l v i r e. Detection of Compromised Online Social Network Account with an Enhanced Knn. – In: Applied Artificial Intelligence. 2020, pp. 777-791.
22. E r e n, M., J. M o o r e, B. A l e x a n d r o. Multi-Dimensional Anomalous Entity Detection via Poisson Tensor Factorization. – In: Proc. of 2020 IEEE International Conference on Intelligence and Security Informatics (ISI'2020), 2020.
23. X i e, R., L. W a n g, X. T a o. A Secure VM Allocation Strategy Based on Tenant Behavior Analysis and Anomaly Identification. – In: Proc. of IEEE Military Communications Conference MILCOM, Vol. **2021-November**, pp. 721-726.
24. Z h a n g, S., F. J i a n g, M. Q i n. Application of System Calls in Abnormal User Behavioral Detection in Social Networks. – In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. **11434**. 2019, LNCS, pp. 89-101.
25. T a o, J., H. W a n g, T. X i o n g. Selective Graph Attention Networks for Account Takeover Detection. – In: Proc. of IEEE International Conference on Data Mining Workshops, ICDMW, Vol. **2018-November**, pp. 49-54.
26. B o a h e n, E., S. F r i m p o n g, M. U j a k p a, R. S o s u, O. L a r b i-S i a w, E. O w u s u, J. A p p a t i, E. A c h e a m p o n g. A Deep Multi-Architectural Approach for Online Social Network Intrusion Detection System. – In: Proc. of 2022 IEEE World Conference on Applied Intelligence and Computing (AIC'2022), 2022, pp. 919-924.
27. M c C o r m i c k, A., W. E b e r l e. Discovering Fraud in Online Classified Ads. – In: Proc. of 26th International Florida Artificial Intelligence Research Society Conference (FLAIRS'2013), 2013, pp. 450-455.
28. S i n g h, K., P. S i n g h, K. K u m a r. User Behavior Analytics-Based Classification of Application Layer HTTP-GET Flood Attacks. – Journal of Network and Computer Applications, Vol. **112**, 2018, pp. 97-114.
29. J a w e d, H., Z. Z i a d, M. K h a n, M. A s r a r. Anomaly Detection through Keystroke and Tap Dynamics Implemented via Machine Learning Algorithms. – Turkish Journal of Electrical Engineering and Computer Sciences, Vol. **26**, 2018, No 4, pp. 1698-1709.
30. R a n j a n, R., S. K u m a r. User Behaviour Analysis Using Data Analytics and Machine Learning to Predict Malicious User Versus Legitimate User. – High-Confidence Computing, Vol. **2**, 2022, No 1.
31. S o m a s u n d a r a m, A., S. R e d d y. Parallel and Incremental Credit Card Fraud Detection Model to Handle Concept Drift and Data Imbalance. – Neural Computing and Applications, Vol. **31**, 2019, pp. 3-14.
32. J i a n g, W., Y. T i a n, W. L i u, W. L i u. An Insider Threat Detection Method Based on User Behavior Analysis. – In: IFIP Advances in Information and Communication Technology. Vol. **538**. 2018, pp. 421-429.
33. K a s a, N., A. D a h b u r a, C. R a v o o r i, S. A d a m s. Improving Credit Card Fraud Detection by Profiling and Clustering Accounts. – In: Proc. of 2019 Systems and Information Engineering Design Symposium (SIEDS'19), IEEE, 2019, pp. 1-6.
34. S h a o, P., J. L u, R. W o n g, W. Y a n g. A Transparent Learning Approach for Attack Prediction Based on User Behavior Analysis. – In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. **9977**. LNCS, 2016, pp. 159-172.
35. A l i m o l a e i, S. An Intelligent System for User Behavior Detection in Internet Banking. – In: Proc. of 2015 4th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS'15), IEEE, 2015, pp. 1-5.

36. K a n g, A., J. W o o, J. P a r k, H. K i m. Online Game Bot Detection Based on Party-Play Log Analysis. – Computers and Mathematics with Applications, Vol. **65**, 2013, No 9, pp. 1384-1395.
37. I l i o u, C., T. K o s t o u l a s, T. T s i k r i k a, V. K a t o s, S. V r o c h i d i s, Y. K o m p a t s i a r i s. Towards a Framework for Detecting Advanced Web Bots. – In: Proc. of 14th International Conference on Availability, Reliability and Security, 2019, pp. 1-10.
38. N g u y e n, P., R. H e n k i n, S. C h e n, N. A n d r i e n k o, G. A n d r i e n k o, O. T h o n n a r d, C. T u r k a y. VASABI: Hierarchical User Profiles for Interactive Visual User Behaviour Analytics. – IEEE Transactions on Visualization and Computer Graphics, Vol. **26**, 2020, No 1, pp. 77-86.
39. G u n a v a t h i, C., R. S w a r n a P r i y a, S. A a r t h y. Big Data Analysis for Anomaly Detection in Telecommunication Using Clustering Techniques. – In: Advances in Intelligent Systems and Computing. Vol. **862**. 2019, pp. 111-121.
40. G a o, M., B. L i, C. W a n g, L. M a, J. X u. User Behavior Clustering Scheme with Automatic Tagging over Encrypted Data. – IEEE Access, Vol. **7**, 2019, pp. 170648-170657.
41. W a n g, Y., Z. Z h a n g, L. C h i. User Account Risk Identification Model for Web Applications. – In: ACM International Conference Proceeding Series, Vol. **Part F148262**, 2019, pp. 30-34.
42. R a z a, S., S. H a i d e r. Suspicious Activity Reporting Using Dynamic Bayesian Networks. – Procedia Computer Science, Vol. **3**, 2011, pp. 987-991.
43. S h e n, H., F. M a, X. Z h a n g, L. Z o n g, X. L i u, W. L i a n g. Discovering Social Spammers from Multiple Views. – Neurocomputing, Vol. **225**, 2017, pp. 49-57.
44. L u z b a s h e v, A., A. F i l i p p o v, K. K o g o s. Continuous User Authentication in Mobile Phone Browser Based on Gesture Characteristics. – In: Proc. of 2nd World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4'2018), 2019, pp. 313-316.
45. Z h a n g, X., Y. H a n, W. X u, Q. W a n g. HOBA: A Novel Feature Engineering Methodology for Credit Card Fraud Detection with a Deep Learning Architecture. – Information Sciences, Vol. **557**, 2021, pp. 302-316.
46. L i, Z., H. Z h a n g, M. M a s u m, H. S h a h r i a r, H. H a d d a d. Cyber Fraud Prediction with Supervised Machine Learning Techniques. – In: Proc. of 2020 ACM Southeast Conference (ACMSE'2020), 2020, pp. 176-180.
47. D i a, D., G. K a h n, F. L a b e r n i a, Y. L o i s e a u, O. R a y n a u d. A Closed Sets Based Learning Classifier for Implicit Authentication in Web Browsing. – Discrete Applied Mathematics, Vol. **273**, 2020, pp. 65-80.
48. Y a n g, H. Research on Classification Algorithm for Civil Aviation Internal Network Intrusion Detection Based on Machine Learning. – In: Proc. of 2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT'2020), 2020, pp. 1-4.
49. u r R a h m a n, A., S. D a s h, A. L u h a c h, N. C h i l a m k u r t i, S. B a e k, Y. N a m. A Neuro-Fuzzy Approach for User Behaviour Classification and Prediction. – Journal of Cloud Computing, Vol. **8**, 2019, No 1.
50. N o c e r a, F., S. D e m i l i t o, P. L a d i s a, M. M o n g i e l l o, A. S h a h, J. A h m a d, E. di S c i a s c i o. A User Behavior Analytics (UBA)-Based Solution Using LSTM Neural Network to Mitigate DDoS Attack in Fog and Cloud Environment. – In: Proc. of 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH'22), 2022, pp. 74-79.
51. S h a r m a, B., P. P o k h a r e l, B. J o s h i. User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder-Insider Threat Detection. – In: ACM International Conference Proceeding Series. 2020.
52. G a n f u r e, G., C.-F. W u, Y.-H. C h a n g, W.-K. S h i h. DeepGuard: Deep Generative User-Behavior Analytics for Ransomware Detection. – In: Proc. of 2020 IEEE International Conference on Intelligence and Security Informatics (ISI'2020), 2020.
53. B u d i a r t o, R., A. A l q a r n i, M. A l z a h r a n i, M. P a s h a, M. F i r d h o u s, D. S t i a w a n. User Behavior Traffic Analysis Using a Simplified Memory-Prediction Framework. – Computers, Materials and Continua, Vol. **70**, 2022, No 2, pp. 2679-2698.
54. H i l a s, C. S., P. A. M a s t o r o c o s t a s. An Application of Supervised and Unsupervised Learning Approaches to Telecommunications Fraud Detection. – Knowledge-Based Systems, Vol. **21**, 2008, No 7, pp. 721-726.

55. W u, Z., L. T i a n, Y. Z h a n g, Z. W a n g. Web User Trust Evaluation: A Novel Approach Using Fuzzy Petri Net and Behavior Analysis. – Symmetry, Vol. **13**, 2021, No 8.
56. L i a n, J. Implementation of Computer Network User Behavior Forensic Analysis System Based on Speech Data System Log. – International Journal of Speech Technology, Vol. **23**, 2020, No 3, pp. 559-567.
57. A i, J., J. W a n g, S. C h e n, H. G u a n, C. L i a n g, L. C h e n. Intelligent Analysis of Database Users Based on a Dynamic Model. – In: Proc. of 2017 2nd International Conference on Machinery, Electronics and Control Simulation (MECS'2017), Atlantis Press, 2016, pp. 146-150.
58. P v, S., S. B h a n u. UbCadet: Detection of Compromised Accounts in Twitter Based on User Behavioural Profiling. – Multimedia Tools and Applications, Vol. **79**, 2020, No 27-28, pp. 19349-19385.
59. U s s a t h, M., D. J a e g e r, F. C h e n g, C. M e i n e l. Identifying Suspicious User Behavior with Neural Networks. – In: Proc. of 4th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud'2017) and 3rd IEEE International Conference of Scalable and Smart Cloud (SSC'2017), 2017, pp. 255-263.
60. H a l a w a, H., M. R i p e a n u, K. B e z n o s o v, B. C o s k u n, M. L i u. An Early Warning System for Suspicious Accounts. – In: Proc. of 10th ACM Workshop on Artificial Intelligence and Security (AISec'2017), Co-Located with CCS, 2017, pp. 51-52.
61. W a n g, Y., L. W a n g. Bot-Like Behavior Detection in Online Banking. – In: ACM International Conference Proceeding Series. 2019, pp. 140-144.
62. O h, J., Z. B o r b o r a, J. S r i v a s t a v a. Automatic Detection of Compromised Accounts in MMORPGs. – In: Proc. of 2012 ASE International Conference on Social Informatics, Social Informatics, 2012, pp. 222-227.
63. K i m, H., S. Y a n g, H. K i m. Crime Scene Re-Investigation: A Postmortem Analysis of Game Account Stealers' Behaviors. – In: Proc. of Annual Workshop on Network and Systems Support for Games, 2017, pp. 1-6.
64. H a l a w a, H., K. B e z n o s o v, B. C o s k u n, M. L i u, M. R i p e a n u. Forecasting Suspicious Account Activity at Large-Scale Online Service Providers. – In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. **11598**. 2019, LNCS, pp. 569-587.
65. H u, Q., B. T a n g, D. L i n. Anomalous User Activity Detection in Enterprise Multi-Source Logs. – In: IEEE International Conference on Data Mining Workshops, ICDMW, Vol. **2017-November**, 2017, pp. 797-803.
66. T a n g, B., Q. H u, D. L i n. Reducing False Positives of User-to-Entity First-Access Alerts for User Behavior Analytics. – In: Proc. of IEEE International Conference on Data Mining Workshops, ICDMW, Vol. **2017-November**, 2017, pp. 804-811.
67. M a t s u s h i t a, H., R. U d a. Detection of Change of Users in SNS by Two Dimensional CNN. – In: Proc. of 2020 IEEE 44th Annual Computers, Software, and Applications Conference, (COMPSAC'2020), 2020, pp. 839-844.
68. B o h a c i k, J., A. F u c h s, M. B e n e d i k o v i c. Detecting Compromised Accounts on the Pokec Online Social Network. – In: Proc. of 2017 International Conference on Information and Digital Technologies (IDT'17), IEEE, 2017, pp. 56-60.
69. Z h a n g, C., Y. H u, X. Z h u, Z. G u o, J. H u a n g. Anomaly Detection for User Behavior in Wireless Network Based on Cross Entropy. – In: Proc. of 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing, 2016, pp. 1258-1263.
70. L e e, S.-C., C. F a l o u t s o s, D.-K. C h a e, S.-W. K i m. Fraud Detection in Comparison-Shopping Services: Patterns and Anomalies in User Click Behaviors. – IEICE Transactions on Information and Systems, Vol. **E100D**, 2017, No 10, pp. 2659-2663.
71. D a r w i s h, S. A Bio-Inspired Credit Card Fraud Detection Model Based on User Behavior Analysis Suitable for Business Management in Electronic Banking. – Journal of Ambient Intelligence and Humanized Computing, Vol. **11**, 2020, No 11, pp. 4873-4887.
72. D a s u, L. S., M. D h a m i j a, G. D i s h i t h a, A. V i v e k a n a n d a n, V. S a r a s v a t h i. Defending Against Identity Threats Using Risk-Based Authentication. – Cybernetics and Information Technologies, Vol. **23**, 2023, No 2, pp. 105-123.

73. A l h e n a w i, E. A., H. A l a z z a m, R. A l-S a y y e d, O. A b u A l g h a n a m, O. A d w a n. Hybrid Feature Selection Method for Intrusion Detection Systems Based on an Improved Intelligent Water Drop Algorithm. – Cybernetics and Information Technologies, Vol. **22**, 2022, No 4, pp. 73-90.
74. L a z a r o v, A. D. Mathematical Modelling of Malware Intrusion in Computer Networks. – Cybernetics and Information Technologies, Vol. **22**, 2022, No 3, pp. 29-47.
75. I m a m, N. H., V. G. V a s s i l a k i s, D. K o l o v o s. An Empirical Analysis of Health-Related Campaigns on Twitter Arabic Hashtags. – In: Proc. of 7th International Conference on Data Science and Machine Learning Applications (CDMA'2022), 1 March 2022, pp. 29-41.
76. G r z e n d a, M., S. K a ź m i e r c z a k, M. L u c k n e r, G. B o r o w i k, J. M a ń d z i u k. Evaluation of Machine Learning Methods for Impostor Detection in Web Applications. – Expert Systems with Applications, Vol. **7**, Juni 2023, 120736.
77. B h a r n e, S., P. B h a l a d h a r e. An Enhanced Scammer Detection Model for Online Social Network Frauds Using Machine Learning – International Journal on Recent and Innovation Trends in Computing and Communication, Vol. **11**, 2023, pp. 239-249,
78. E r e n, M. E., J. S. M o o r e, E. S k a u, E. M o o r e, M. B h a t t a r a i, G. C h e n n u p a t i, B. S. A l e x a n d r o v. General-Purpose Unsupervised Cyber Anomaly Detection via Non-Negative Tensor Factorization. – Digital Threats: Research and Practice, Vol. **4**, 7 Mar 2023, No 1, pp. 1-28.
79. S i n g h, M., B. M. M e h t r e, S. S a n g e e t h a, V. G o v i n d a r a j u. User Behaviour Based Insider Threat Detection Using a Hybrid Learning Approach. – Journal of Ambient Intelligence and Humanized Computing, Vol. **14**, April 2023, No 4, pp. 4573-4593.

Received: 05.07.2023; Second Version: 07.08.2023; Accepted: 18.08.2023 (fast track)