applied sciences

MDPI

Article

Users' Reaction Time for Improvement of Security and Access Control in Web Services

Shamil Magomedov [1], Alexander Gusev [2,3], Dmitry Ilin [1] and Evgeny Nikulchev [1,*]

[1] Department of Intelligent Information Security Systems, MIREA—Russian Technological University, 119454 Moscow, Russia; magomedov_sh@mirea.ru (S.M.); i@dmitryilin.com (D.I.)
[2] Data Center, Russian Academy of Education, 119121 Moscow, Russia; alexander.gusev@rusacademedu.ru
[3] Kuban State Technological University, 350072 Krasnodar, Russia
* Correspondence: nikulchev@mail.ru

Abstract: This paper concerns the case of the development of a technology for increasing the efficiency of access control based on the user behavior monitoring built into a software system's user interface. It is proposed to use the time of user reactions as individual indicators of psychological and psychophysical state. This paper presents the results and interpretation of user reactions collected during a mass web survey of students of the Russian Federation. The total number of users was equal to 22,357. To reveal the patterns in user reactions, both quantitative and qualitative approaches were applied. The analysis of the data demonstrated that the user could be characterized by their psychomotor reactions, collected during the answering of a set of questions. Those reactions reflected the personal skills of the interface interaction, the speed of reading, and the speed of answering. Thus, those observations can be used as a supplement to personal verification in information systems. The collection of the reaction times did not load the data volumes significantly nor transmit confidential information.

Keywords: big data; analysis of user reactions; patterns in user reactions; personal verification in information systems

Citation: Magomedov, S.; Gusev, A.; Ilin, D.; Nikulchev, E. Users' Reaction Time for Improvement of Security and Access Control in Web Services. *Appl. Sci.* **2021**, *11*, 2561. https://doi.org/10.3390/app11062561

Academic Editor: Ugo Vaccaro

Received: 14 February 2021
Accepted: 11 March 2021
Published: 12 March 2021

1. Introduction

The direction of digitalization is characterized by the transformation of government [1], health [2], educational [3], banking, etc., services [4] and economic relations in general [5] into the form of web services.

Developers need to solve the problem of a contradiction. On the one hand, the computing service should be as accessible as possible, platform independent, convenient, and easy to use [6]. If the service, for example, is provided in "one click," access should not take a lot of time. On the other hand, the services provided in the context of digitalization are associated with a large amount of personal, medical, banking, and other confidential data [7], the protection of which requires significant efforts. To ensure secure access control, information security technologies are used [8], which, as a rule, are external to the used software and hardware infrastructure of information support of services [9]. This approach has a negative impact on the characteristics of the system. It can slow down the work of services when working with big data [10], limit the number of users, and leave the possibility of programmatically unauthorized access for developers and administrators. If security systems are not considered when designing a web service, then their external connection at the level of protection for users, applications, computer data transmission networks, data storage systems, and servers of a computing complex significantly decreases the technical characteristics of quality and reliability.

Public web services have several features that cannot be considered when controlling access to data based on the use of external information security tools [11]. This is the transfer of passwords to third parties, the interception of passwords by malicious software,

or conditions in which a user who has gone through all conceivable and inconceivable verification methods knowingly or accidentally left the system active (did not close the web page or account) and another user began to interact with the service, thus gaining access to confidential information [12]. To develop access control, it is required to use built-in tools for confirming the identity of the user in the process of interaction [13]. In antifraud banking systems, methods for analyzing suspicious transactions are used. In systems with increased confidentiality, methods for analyzing user behavior are used.

Contemporary interdisciplinary studies in the field of psychology and psychodiagnostics using web tools and various devices make it possible to diagnose the psychometric data of users and control their change in the process of interacting with the web interface.

This paper is devoted to the development of a technology for increasing the efficiency of access control based on the user behavior monitoring built into the software system's user interface for assessing the time of user reactions as individual indicators of psychological and psychophysical state.

The paper consists of six sections. The section "Related Works" (Section 2) sets out related issues of the study. The section "Technologies and Methods" (Section 3) describes methods for conducting experiments and methods for constructing a system architecture with user behavior analysis. The "Experiment" section (Section 4) describes the results of experimental studies. The "Discussion" section (Section 5) discusses the results obtained. In the section "Conclusion" (Section 6), general conclusions and perspectives of the research directions are given.

2. Related Works

Currently, computing architectures are being developed based on the concept of Security Information and Event Management (SIEM [14], which combines real-time event monitoring and information security management. SIEM systems are being deployed over protected information systems and presented in the form of integrated devices or multicomponent complexes. There are commercial solutions for SIEM systems such as QRadar IBM, Arc Sight HP, Symantec Security Services, FortiSIEM, etc. A significant number of contemporary studies are devoted to the development of SIEM system architectures: identification of threat sources, and mechanisms for their detection in distributed systems [15], blocking of malicious traffic from IoT devices [16], intelligent data processing from multiple sources [17,18], the use of event classification methods [19], etc.

For web services, one of the ways is to use role-based access control, where each entry point is associated with a set of user roles [20]. Various research groups have presented context-sensitive approaches and access control frameworks that differ in their context models, policy models, and reasoning capabilities [21]. Several role-based access control models have been proposed [22–24], incorporating dynamically changing contextual conditions (e.g., user- and resource-centric information) into policies. Similar to the spatial and temporal approaches [25–27], these context-sensitive approaches are mainly domain specific and take into account specific types of contextual conditions. A context-sensitive approach to role-based access control has been developed [28,29] to facilitate access control to data resources based on a wide range of contextual conditions.

Adding UBA (User behavioral analytics) tools [30] to SIEM capabilities provides the means for behavioral analysis of users and entities (processes, hosts, network activities). The main difference between SIEM and UEBA (User and entity behavioral analytics) is that the SIEM system acts as a kind of constructor for collecting logs, and the UEBA solution builds behavioral models [31]. Algorithms for finding and processing anomalies can include various methods that tell the operator which users and entities in the network began to behave atypically and why this behavior is atypical for them. Such systems are implemented by embedding dynamic models into web applications; they include situational models and tools for their interpretation [32].

However, it seems appropriate to use psychomotor reactions [33–35] to work with questionnaires or simple questions [13]. In [36], a data set with an analysis of user reactions when working with polls is published and the possibility of their personalization is shown.

3. Technologies and Methods

It is proposed to develop a technology for the implementation of the multilevel protection architecture that would use the user's reaction time when working with the web interface as an additional user identifier. In this case, data collection will be carried out by built-in software components and interface elements, and afterwards, the data will be transferred to the system.

Figure 1 shows the case when "User 1" has entered all the necessary data for access but can be replaced by another user from the workstation of "User 1" as well as from another place. If there are no blocks in the system related to user behavior and location, "User 2" can access the data.

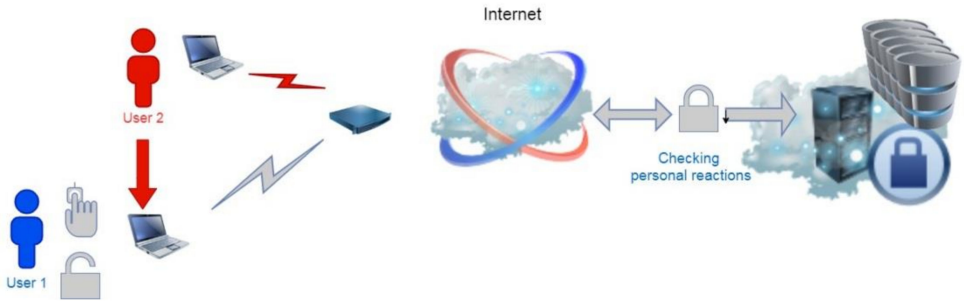

Figure 1. Example of the system with access control.

It is proposed to include a number of verification questions into the access control system. In this case, it is possible to take into account not only the answer to a specific verification question, but also the reaction time. This will allow excluding cases of changing the user in a single session using personal reactions. It is also possible to define a user when using someone else's passwords to enter the system. Possible cases with a reaction change caused by the current psychoemotional state require additional confirmation of the user's identity. So, in cases, for example, of illness or a decrease in the concentration of the user, the user's admission can be checked by special services in systems with strict access policies.

In general, the technology being developed can be represented as follows:

1. The technology is implemented by a computing complex. It can provide a client with one or more services, such as, for example, event monitoring services, financial services, banking services, government services, educational services, real-time data transmission services, gaming services, search services, etc.
2. The system includes computer networks, data transmission control systems (that is, the environment used to provide communication channels between computers), data processing systems, and other devices. The network can include connections in the form of wired communication lines, wireless communication channels, and fiber optic cables.
3. The system can send security incidents to the cloud platform for further analysis by a machine learning application based on the identified characteristics of security incidents detected during local analysis using the security module and event manager. The characteristics identified can include, for example, information that the observed parameters have a safety risk assessment above a threshold value.
4. The infrastructure creates a persistent repository of security information and an event manager. For example, it could be a security information and event manager, which can be implemented as a hardware component or a combination of hardware and

software components. The information and security events manager controls the process of selecting only specific security incidents for local and remote analysis.

5. The interval for evaluating the psychomotor reactions of the user is a predetermined time interval on the basis of which security incidents are formed.

The workload layer provides the functionality for which systems are used. The collection of behavior characteristics should be built into the interface of client applications. So, for systems [37] that imply the transfer of state, it is necessary to collect data on user requests to the API, tracking the time, parameters, and user ID, and for systems with a graphical user interface (GUI), to collect data on actions regarding the interface, tracking the time of action and user identifiers.

In the process of the user working with the system interface, it is necessary to check the transition conditions based on the previously completed sets of actions recorded in the event.

4. Experiment

The studies were carried out using the digital platform DigitalPsyTools [38,39]. The system is both a digital platform with a web interface and a psychodiagnostic tool used for population research in the education system. Platform-independent evaluation functions are built into the elements of its web interface.

Between the application of an external stimulus and the corresponding motor response, there is a certain period of time for the stimulus, called the reaction time.

Estimation of this time is one of the important methods of studying the rate of cognitive processing of information by a person and the coordinated response of peripheral movements.

Many factors affect the reaction time, such as age, physical condition, fatigue, health, etc. Longer response times mean reduced productivity. For this study, the reaction time is the timespan from the start of the web page presentation on which an action can be taken to the time when the user performed this action in the interface. In other words, reaction time is the timespan from the stimulus appearance to the moment when the user presses the corresponding button (based on psychological terms).

The fragment of a large psychological survey among first-year students from 20 different universities is presented. During the survey, students answered various questionnaires and passed cognitive tests; at the same time, a study was organized on the built-in reactions to answers to simple questionnaire questions. Not only was the answer recorded, but also the time spent on the answer, including reading the question and choosing the answer in the presented web interface.

The hypothesis was that reaction times of different responses with different user interface elements are personal. The hypothesis of the analysis of data on the reaction time consisted of the possibility of determining the dependence in the reactions of users when working with interface elements when answering a question asked, as well as the possibility of determining individual psychomotor reactions when working with the interface.

During the survey, students were presented with the following three questions, among others:

1. Study program (choice of four options: bachelor's/master's/specialty/postgraduate study).
2. Basis of training (choice from three options: budget/contract/target).
3. Indicate the profile of your education (choice from four options: technical/humanitarian/natural science/no profile).

Questions 1 and 2 were asked at the beginning of the survey. Question 3 was asked one hour after the survey began.

The questionnaire is organized as a web interface. After receiving the polled archive, it is unpacked and downloaded to the browser on the client's device. In each element of the survey, the answer and the response time are recorded in milliseconds (from the moment of loading until the choice of the answer and pressing the button "next"), i.e., the time during which the user read the question, considered the given options and selected the

appropriate option. The survey was large and included cognitive tests, and the user was interested in going to the next page. Data were transferred to the platform after the end of the entire survey or after the user closed the web page. This ensured that the networks did not interfere with the response time estimation.

The total number of students who participated in the survey was equal to 23,102. Figure 2 demonstrates the histograms of the reaction time to Questions 1–3.

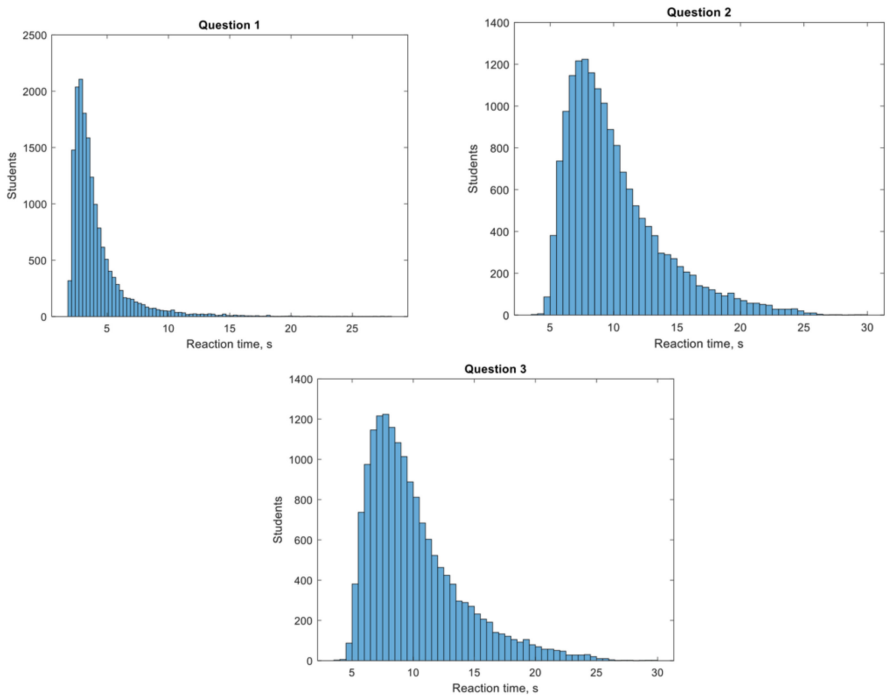

Figure 2. Histograms of reaction time to Questions 1–3.

Records containing empty answers or reaction times lower than 2 s were withdrawn from the dataset. The remaining 22,357 records were normalized, and the mean values for each question were calculated. Then, the new dataset was generated containing the deviation from the mean reaction time for each student according to each question. That dataset of deviations was then processed as the object for analysis.

To assess the students' reaction time deviations qualitatively, we introduced a scale dividing the deviations into four quartiles in ascending order. Thus, each of 22,357 students had an ordered triad like (1, 2, 4) representing them with respect to their reaction time deviations for Questions 1–3. The borders for the quartiles are shown in Table 1.

Table 1. The borders for the quartiles of reaction time deviations.

	Quartile 1	Quartile 2	Quartile 3	Quartile 4
		Question 1		
Lower border	0	0.0056	0.0063	0.0068
Upper border	0.0055	0.0062	0.0067	1
		Question 2		
Lower border	0	0.0053	0.0071	0.0082
Upper border	0.0052	0.007	0.0081	1
		Question 3		
Lower border	0	0.0075	0.011	0.014
Upper border	0.0074	0.0109	0.013	1

The quantitative analysis of the reaction time deviations data shows the significant correlation between the deviations in answering Questions 1–3. The correlation coefficients are presented in Table 2.

Table 2. The coefficients of correlation between reaction time deviations of the students for the questions 1–3. Arguments 1–3 stand for the number of the question.

R (1,2)	R (1,3)	R (2,3)
0.9298	0.8039	0.8376

During the studying of the interaction between the reaction times deviation for the three questions, the Wald test [40] was performed (Table 3), demonstrating the significant linear interdependence between the deviations.

Table 3. The Wald test statistics for the deviations D_1-D_3 of reaction times for Questions 1–3, respectively, at the significance level of 0.05, β_1, β_3 are the constant values, and ε is the normally distributed error with a mean of 0 and a variance of 1.

Unrestricted Model	Restrictions	Wald Statistics	Critical Value
$D_1 = \beta_0 + \beta_1 D_2 + \beta_2 D_3 + \varepsilon$	$\beta_1 = 0,\ \beta_2 = 0$	145,320	5.9915
$D_1 = \beta_0 + \beta_1 D_2 + \varepsilon$	$\beta_1 = 0$	142,700	3.8415
$D_1 = \beta_0 + \beta_2 D_3 + \varepsilon$	$\beta_2 = 0$	40,854	3.8415
$D_2 = \beta_0 + \beta_1 D_1 + \beta_2 D_3 + \varepsilon$	$\beta_1 = 0,\ \beta_2 = 0$	176,340	5.9915
$D_2 = \beta_0 + \beta_2 D_3 + \varepsilon$	$\beta_2 = 0$	52,547	3.8415
$D_3 = \beta_0 + \beta_1 D_1 + \beta_2 D_2 + \varepsilon$	$\beta_1 = 0,\ \beta_2 = 0$	53,735	5.9915

During the qualitative analysis, it was discovered that 17,002 or 76% of students belonged to the same quartile in all the three questions or no more than one their quartile was next to the other two (Table 4).

Table 4. Frequency of the triads with no or minor qualitative differences between reaction time deviations to questions.

Triad	No. of Occurrences	Triad	No. of Occurrences
(1 1 1)	2156	(2 3 3)	1015
(2 2 2)	983	(3 2 2)	567
(3 3 3)	1313	(3 2 3)	425
(4 4 4)	2734	(3 3 2)	410
(1 1 2)	985	(3 3 4)	383
(1 2 1)	409	(3 4 3)	335
(1 2 2)	690	(3 4 4)	774
(2 1 1)	632	(4 3 3)	538
(2 1 2)	412	(4 3 4)	232
(2 2 1)	476	(4 4 3)	501
(2 2 3)	643		
(2 3 2)	389	Total	17,002 out of 22,357

5. Discussion

The experiment to measure user reactions was carried out as a part of a large psychological study. First-year students from 20 different universities from different cities of the Russian Federation took part in this study, which consisted of surveys and research in the form of cognitive tests. The assessment of reactions to simple questions was built into the survey. The respondents used different devices and types of browsers. A fragment of the

dataset and the analysis of devices are given in the dataset description in the work [36]. The obtained histograms indicate the reliability of the experiment.

Questions 1 and 2 considered in this article were at the beginning of the web survey, and Question 3 was answered after about 1 h, after passing the tasks related to the assessment of spatial abilities; that is, the respondents to the answer to Question 3 were already tired. However, from the obtained histograms and the presented results, it can be seen that despite the change in the reaction time for all data, for all users, the user reactions remained unchanged; that is, both at the beginning of working with the environment and after fatigue, users, on average, demonstrated their characteristic interactions with the interface. This includes the reading speed, the processing time of the data by the nervous system, and corresponding user interface interactions; that is, for those who are slow with information perception and processing, the same degree of inertness remains constant during the study, relative to the average value for all experimental data. Therefore, we built correlations between the values of the deviations of the user's reaction from the average for this issue. The results show that the correlations are high. The data were split into quartiles based on user reaction. A total of 17,000 out of 22,000 subjects showed fell into the same or neighboring quartile. This seems like a high enough value.

To assess the possibility of predicting reactions, the possibilities of constructing regression dependencies were checked, and the Wald test was carried out. It was found that dependencies can be built. This result allows building predictive values of user reactions. This is essential for the considered problem of access control. For example, to check whether a verified user is working with the system, a secret question or other simple question with personal data is asked. Analysis of the user's reaction to the answer to this question is also personal information. The safety control system can compare the predicted value with the received value. Wald's test showed that simple models can be significant; that is, checking and calculating a forecast does not require a significant amount of resources for data processing, which compares favorably with systems for analyzing user behavior based on resource-intensive methods, such as intelligent ones.

Thus, the study demonstrates confirmation of the hypothesis about personal user reactions.

Analysis of user reactions is applicable to confirm the identity of the user during the interaction with the system [41]. This allows detecting the unwanted situations of the collective use of accounts, as well as capturing access by intruders. Analysis of the user behavior relying on the approaches that imply the training of ML models on legal user actions allows detecting deviations from the normal interaction pattern caused by the intervention of third-party users and intruders.

6. Conclusions

The analysis of user behavior for security systems is one of the promising areas in the development of computer systems. In the long term, this approach will prevent attackers from taking possession of confidential information when a verified user forgets to close the session, while not distracting the respectable user with constant distractions in the form of confirming their identity. There is a lot of research in this direction based on the analysis of user psychology.

This research aimed at analyzing the connection between the user's psychology and skills in interacting with information systems. The study is based on testing the hypothesis about the personal reactions of users when interacting with the web interface. The hypothesis was confirmed as a result of an experiment conducted with more than 22,000 respondents.

It should be noted that user reactions can change over time; the user gets used to a particular system, and reactions can be improved. In this case, in the access control system, it is necessary to periodically calibrate personal values in the conditions of other access control systems; for example, biometrics. In situations where the user, for example, has suffered an illness associated with psychosomatics, their reactions can be greatly changed. All this requires additional research in the future. However, it is possible to record the first

few reactions in the current session in the system and build predictive models based on them. According to our research, this seems to be possible.

In situations where the user has felt a strong deterioration in the process of work, the action of the security system depends on the type of system. If the system requires increased security, then perhaps the user in this state needs to stop accessing the data. If, for example, in the user's office, reactions have worsened greatly, the security service can make sure that the user is the same and decide to continue working or provide assistance. In any case, such an access control message is the source for the security response.

Thus, this study was carried out to provide a basis for building access control systems for analyzing reaction time during user interface interactions. An important advantage of such systems is the low resource requirements for collecting and transferring data, as well as for building simple regression models.

Clustering data using artificial intelligence is a subject of future research. The use of reactions when analyzing interface elements for user groups forms a new important use case of users' telemetry data.

Author Contributions: Conceptualization, S.M. and E.N.; methodology, S.M.; software, D.I.; validation, A.G., E.N. and S.M.; formal analysis, A.G.; data curation, D.I.; writing—original draft preparation, S.M.; writing—review and editing, E.N.; visualization, A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of Science and Higher Education of the Russian Federation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gil-Garcia, J.R.; Flores-Zúñiga, M.Á. Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. *Gov. Inf. Q.* **2020**, *37*, 101518. [CrossRef]
2. Lewinter, K.E.; Hudson, S.M.; Kysh, L.; Lara, M.; Betz, C.L.; Espinoza, J. Reconsidering reviews: The role of scoping reviews in digital medicine and pediatrics. *NPJ Digit. Med.* **2020**, *3*, 1–4. [CrossRef]
3. Emejulu, A.; McGregor, C. Towards a radical digital citizenship in digital education. *Crit. Stud. Educ.* **2019**, *60*, 131–147. [CrossRef]
4. Rasool, A.; Shah, F.A.; Islam, J.U. Customer engagement in the digital age: A review and research agenda. *Curr. Opin. Psychol.* **2020**, *36*, 96–100. [CrossRef] [PubMed]
5. Elia, G.; Margherita, A.; Passiante, G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. *Technol. Forecast. Soc. Chang.* **2020**, *150*, 119791. [CrossRef]
6. Li, F.; Lu, H.; Hou, M.; Cui, K.; Darbandi, M. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technol. Soc.* **2021**, *64*, 101487. [CrossRef]
7. De Hert, P.; Papakonstantinou, V.; Malgieri, G.; Beslay, L.; Sanchez, I. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Comput. Law Secur. Rev.* **2018**, *34*, 193–203. [CrossRef]
8. El Sibai, R.; Gemayel, N.; Bou Abdo, J.; Demerjian, J. A survey on access control mechanisms for cloud computing. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3720. [CrossRef]
9. Al-Shargabi, B.A.S.S.A.M.; AlJawarneh, S.H.A.D.I.; Hayajneh, S.M. A cloudlet based security and trust model for e-government web services. *J. Theor. Appl. Inf. Technol.* **2020**, *98*, 27–37.
10. Sheng, J.; Amankwah-Amoah, J.; Wang, X. Technology in the 21st century: New challenges and opportunities. *Technol. Forecast. Soc. Chang.* **2019**, *143*, 321–335. [CrossRef]
11. Cai, F.; He, J.; Ali Zardari, Z.; Han, S. Distributed management of permission for access control model. *J. Intell. Fuzzy Syst.* **2020**, *38*, 1539–1548. [CrossRef]
12. Yarmand, M.H.; Sartipi, K.; Down, D.G. Behavior-based access control for distributed healthcare systems. *J. Comput. Secur.* **2013**, *21*, 1–39. [CrossRef]
13. Bosnjak, M.; Tuten, T.L.; Wittmann, W.W. Unit (non) response in web-based access panel surveys: An extended planned-behavior approach. *Psychol. Mark.* **2005**, *22*, 489–505. [CrossRef]

14. El Arass, M.; Souissi, N. Smart SIEM: From big data logs and events to smart data alerts. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 3186–3191.
15. Kufel, L. Security event monitoring in a distributed systems environment. *IEEE Secur. Priv.* **2013**, *11*, 36–43. [CrossRef]
16. Al-Duwairi, B.; Al-Kahla, W.; AlRefai, M.A.; Abdelqader, Y.; Rawash, A.; Fahmawi, R. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 2182–2191. [CrossRef]
17. Lee, J.; Kim, J.; Kim, I.; Han, K. Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access* **2019**, *7*, 165607–165626. [CrossRef]
18. Moukafih, N.; Orhanou, G.; El Hajji, S. Neural Network-Based Voting System with High Capacity and Low Computation for Intrusion Detection in SIEM/IDS Systems. *Secur. Commun. Netw.* **2020**, *2020*, 3512737. [CrossRef]
19. Sancho, J.C.; Caro, A.; Ávila, M.; Bravo, A. New approach for threat classification and security risk estimations based on security event management. *Future Gener. Comput. Syst.* **2020**, *113*, 488–505. [CrossRef]
20. Walker, A.; Svacina, J.; Simmons, J.; Cerny, T. On automated role-based access control assessment in enterprise systems. In *Information Science and Applications*; Springer: Singapore, 2020; pp. 375–385. [CrossRef]
21. Nyame, G.; Qin, Z. Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework. *Information* **2020**, *11*, 334. [CrossRef]
22. Kirrane, S.; Mileo, A.; Decker, S. Access control and the resource description framework: A survey. *Semant. Web* **2017**, *8*, 311–352. [CrossRef]
23. Schefer-Wenzl, S.; Strembeck, M. Modelling context-aware RBAC models for mobile business processes. *Int. J. Wirel. Mob. Comput.* **2013**, *6*, 448–462. [CrossRef]
24. Trnka, M.; Cerný, T. On security level usage in context-aware role-based access control. In Proceedings of the SAC, Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016; pp. 1192–1195.
25. Bertino, E.; Bonatti, P.A.; Ferrari, E. TRBAC: A temporal role-based access control model. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2001**, *4*, 191–233. [CrossRef]
26. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]
27. Yin, X.C.; Liu, Z.G.; Ndibanje, B.; Nkenyereye, L.; Riazul Islam, S.M. An IoT-based anonymous function for security and privacy in healthcare sensor networks. *Sensors* **2019**, *19*, 3146. [CrossRef] [PubMed]
28. Kayes, A.S.M.; Kalaria, R.; Sarker, I.H.; Islam, M.; Kumara, I. A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. *Sensors* **2020**, *20*, 2464. [CrossRef] [PubMed]
29. Kayes, A.S.M.; Rahayu, W.; Dillon, T.; Chang, E.; Han, J. Context-aware access control with imprecise context characterization for cloud-based data resources. *Future Gener. Comput. Syst.* **2019**, *93*, 237–255. [CrossRef]
30. Akutota, T.; Choudhury, S. Big data security challenges: An overview and application of user behavior analytics. *Int. Res. J. Eng. Technol.* **2017**, *4*, 1544–1548.
31. Xi, X.; Zhang, T.; Ye, W.; Wen, Z.; Zhang, S.; Du, D.; Gao, Q. An Ensemble Approach for Detecting Anomalous User Behaviors. *Int. J. Softw. Eng. Knowl. Eng.* **2018**, *28*, 1637–1656. [CrossRef]
32. Mironov, V.; Gusarenko, A.; Yusupova, N.; Smetanin, Y. Json documents processing using situation-oriented databases. *Acta Polytech. Hung.* **2020**, *17*, 29–40. [CrossRef]
33. Kim, J.; Gabriel, U.; Gygax, P. Testing the effectiveness of the Internet-based instrument PsyToolkit: A comparison between web-based (PsyToolkit) and lab-based (E-Prime 3.0) measurements of response choice and response time in a complex psycholinguistic task. *PLoS ONE* **2019**, *14*, e0221802. [CrossRef] [PubMed]
34. Anrijs, S.; Ponnet, K.; De Marez, L. Development and psychometric properties of the Digital Difficulties Scale (DDS): An instrument to measure who is disadvantaged to fulfill basic needs by experiencing difficulties in using a smartphone or computer. *PLoS ONE* **2020**, *15*, e0233891. [CrossRef]
35. Magomedov, S.G.; Kolyasnikov, P.V.; Nikulchev, E.V. Development of technology for controlling access to digital portals and platforms based on estimates of user reaction time built into the interface. *Russ. Technol. J.* **2020**, *8*, 34–46. [CrossRef]
36. Magomedov, S.; Ilin, D.; Silaeva, A.; Nikulchev, E. Dataset of user reactions when filling out web questionnaires. *Data* **2020**, *5*, 108. [CrossRef]
37. Nikulchev, E.; Kolyasnikov, P.; Ilin, D.; Kasatonov, S.; Biryukov, D.; Zakharov, I. Selection of Architectural Concept and Development Technologies for the Implementation of aWeb-Based Platform for Psychology Research. *Adv. Intell. Syst. Comput.* **2019**, *858*, 672–685.
38. Nikulchev, E.; Ilin, D.; Kolyasnikov, P.; Belov, V.; Zakharov, I.; Malykh, S. Programming technologies for the development of web-based platform for digital psychological tools International. *J. Adv. Comput. Sci. Appl.* **2018**, *9*, 34–45.
39. Nikulchev, E.; Ilin, D.; Silaeva, A.; Malykh, S. Digital Psychological Platform for Mass Web-Surveys. *Data* **2020**, *5*, 95. [CrossRef]
40. Liu, X. *Methods and Applications of Longitudinal Data Analysis*, 1st ed.; Elsevier: Amsterdam, The Netherlands, 2015.
41. Magomedov, S.; Lebedev, A. Protected Network Architecture for Ensuring Consistency of Medical Data through Validation of User Behavior and DICOM Archive Integrity. *Appl. Sci.* **2021**, *11*, 2072. [CrossRef]