International Journal on Applications in Information and Communication Engineering
Volume 9 : Issue 4 : September 2023, pp15 – 22 www.aetsjournal.com ISSN (Online) : 2394 - 6237

DESIGN OF AN IOT-BASED RANKING SECURITY SYSTEM USING THE SHA3 256 ALOGRITM

M KATHIRVEL, D THIRUPATHI, A SURESH KUMAR, S POORNA PRAKASH

Department Of Computer Science and Engineering- Regional Language
Rathinam Technical Campus, Coimbatore.

Abstract - The process for creating such security rankings for home consumer electronics in a methodical manner. It can be used with data from any type of security assessment study. When seen through the lens of the Internet of Things, this report presents a comprehensive survey of security vulnerabilities in smart home consumer devices. AHP model for ranking commonly used home consumer devices such as home theatres, security cameras, smart lighting, smart speakers, video surveillance, smart switches, home automation systems, home security systems, smart routers, wireless doorbell cameras, and home audio systems was developed using this methodology. This research presents a fresh way for creating such security rankings for home consumer electronics in a systematic manner. Any data from a security assessment study can be used to implement the proposed methodology. Previous attempts to apply Analytic Hierarchy are discussed in this study.

Key Words: Cloud Computing,

1.INTRODUCTION

1.1THE SMART HOUSE

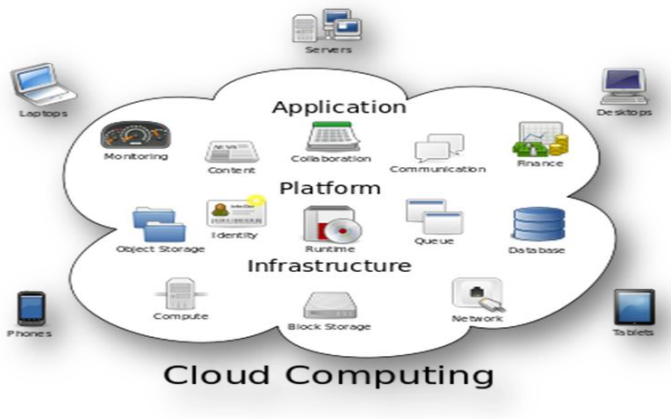
Protecting the privacy of information embedded in a home environment, maintaining the confidentiality and integrity of customer data, and assuring the availability of smart home services 24 hours a day, seven days a week are all part of smart home security. Consumers are typically aware of the security concerns involved with consumer gadgets and are prepared to pay for such devices to be labelled with security labels. As a result, IoT consumer device security labelling should clearly indicate security measures (e.g., security updates, access control, and encryption).

1.2 APPLICATIONS FOR CONSUMERS

Consumer IoT applications are proving to be a substantial market with a high volume of sales. Smart watches, electronics, television sets, virtual reality, and health tracking are among the most popular purchases. The Internet of Things (IoT) makes life easier, and more people are buying devices to control and monitor it.

What is cloud computing and how does it work?

The utilization of computing resources (hardware and software) offered as a service through a network is known as cloud computing (typically the Internet). The name stems from the widespread use of a cloud-shaped symbol in system diagrams as a metaphor for the complicated architecture it encompasses. Cloud computing entrusts a user's data, software, and processing to remote services. Cloud computing refers to the use of managed third-party services to make hardware and software resources available over the Internet. Typically, these services provide access to powerful software programmed and high-end server computer networks.



What is Cloud Computing and How Does It Work?

The goal of cloud computing is to use traditional supercomputing, or high-performance computing power, which is typically used by military and research facilities to perform tens of trillions of computations per second in consumer-oriented applications like financial portfolios, personalized information, data storage, and the power to run large, immersive computer games. Cloud computing distributes data-processing tasks across a network of large groups of machines, often using low-cost consumer PC technology with specialized connections.

This shared IT infrastructure consists of big groups of interconnected systems. Virtualization techniques are frequently utilized to boost the power of cloud computing.

2. LITERATURE SURVEY

An Analysis of IoT Devices on Home Networks Author: Deepak Kumar, Kelly Shen, Deepali Garg**.** In this paper, we provide the first large-scale empirical analysis of IoT devices in real-world homes by leveraging data collected from user-initiated network scans of 83M devices in 16M households. We find that IoT adoption is widespread: on several continents, more than half of households already have at least one IoT device. Device types and manufacturer popularity vary dramatically across regions. For example, while nearly half of North American homes have an Internet-connected television or streaming device, less than three percent do in South Asia where the majority of devices are surveillance cameras. We investigate the security posture of devices, detailing their open services, weak default credentials, and vulnerability to known attacks. Device security similarly varies geographically, even for specific manufacturers. For example, while less than 17% of TP-Link home routers in North America have guessable passwords, nearly half do in Eastern Europe and Central Asia. We argue that IoT devices are here, but for most homes.

Taxonomy of cyber security metrics to measure strength of cyber security . Author: Seema Gupta Bohol, JR Mohanty, Prasant, Kumar Patnaik**.** Cyber security is guarding computer systems, data, network and other resources from unauthorized access and malicious users. There are no direct methods of measuring strength of cyber security. As they say, "You can't manage what you can't measure". One can easily track the efforts taken for security through cyber security metrics. Being a quantifiable measure, metric can be utilized in tracking the status of a specific process and assess its outcomes along with its strength. This work aims to provide taxonomy of cyber security metrics with five basic metrics, along with the tools under Multi Criteria Decision making approach can be used in evaluation of cyber security strength**.**

3. EXISTING SYSTEM

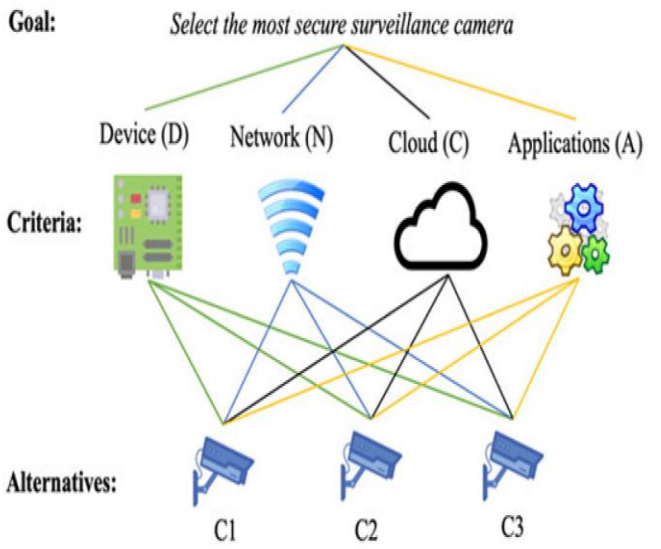
Consumers are typically aware of the security concerns connected with consumer gadgets and are prepared to pay for such devices to be labeled with security labels. IoT consumer device security labels that indicate security methods (e.g., security updates, access control, encryption), data practices (e.g., whether data is saved on the device or in the cloud), and extra information (e.g., physical actuation).Because of a variety of interacting factors such as device hardware, networking, middleware, and so on, determining the relative security of a type of consumer device is a complex Multi-Criteria Decision-Making (MCDM) problem, determining the relative security of a type of consumer device is a complex Multi-Criteria Decision-Making (MCDM) problem. For each level, a comparison matrix is built based on pairwise comparisons. Following that, the AHP algorithm prioritizes each criterion and sub-criteria in the hierarchy.

3.1 SYSTEM PROPOSED

To create AHP hierarchies to assess security in a variety of computer-related fields. Congeniality, integrity, authentication, and availability are the most common security criteria. In this methodology, AHP is used to produce security rankings for smart home devices. The four top-level criteria of device, network, cloud, and application security are shown in a simplified example of how AHP may be used to rank device security utilizing the IoT lens and the four top-level criteria of the device, network, cloud, and application security. Using an AHP based on security requirements for devices, networks, clouds, and applications. For the sake of simplicity, lower-level sub-criteria are not included.

3.2 SYSTEM ARCHITECTURE

A system architecture is the conceptual model that defines the structure, behavior, and more views of a system.
An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.



4 MODULE DESCRIPTION

4.1 Dataset Collection

The datasets we used in this study are open source and freely available online. The data includes both fake and truthful news articles from multiple domains. The truthful news articles published contain true description of real world events, while the fake news websites contain claims that are not aligned with facts. The conformity of claims from the politics domain for many of those articles can be manually. We have used three different datasets in this study, a brief description of which is provided as follows.The first dataset is available at Kaggle (hereafter referred to as DS2) which contains a total of 20,386 articles used for training and 5,126 articles used for testing. The dataset is built from multiple sources on the Internet. The articles are not limited to a single domain such as politics as they include both fake and true articles from various other domains.

4.2 Data Storage

Two data sets can have the same mean but they can be entirely different. Thus to describe data, one needs to know the extent of variability. This is given by the measures of store. Range, interquartile range, and standard deviation are the three commonly used measures of store.

4.3 Encryption

There are two basic encryption algorithms for cloud-based data: Symmetric encryption: The encryption and decryption keys are the same. This method is most commonly used for bulk data encryption.

4.4 Verification

A practical authentication product should be relatively quick to use. Users should not feel that the verification procedure increases their work load or distracts their work. Therefore we are interested in the time of the actual use of the authentication system. In the third stage, we discard the authentication products that result in an unacceptably time consuming authentication process. The authentication product usability is computed from the estimated annual time consumption

4. 5 Authentication

This module is used to control the trade between the sellers and the buyers. It also control the user registration process.This module is responsible for the data verification, data encryption, etc.

UML DIAGRAMS

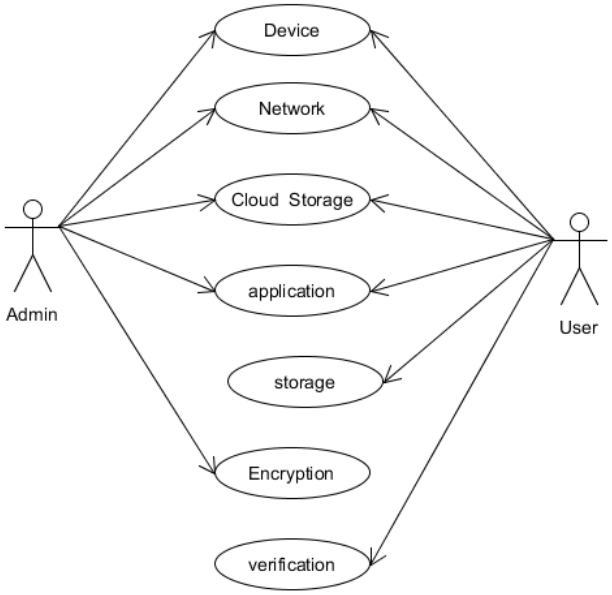
UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering.
The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object oriented computer software.

In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

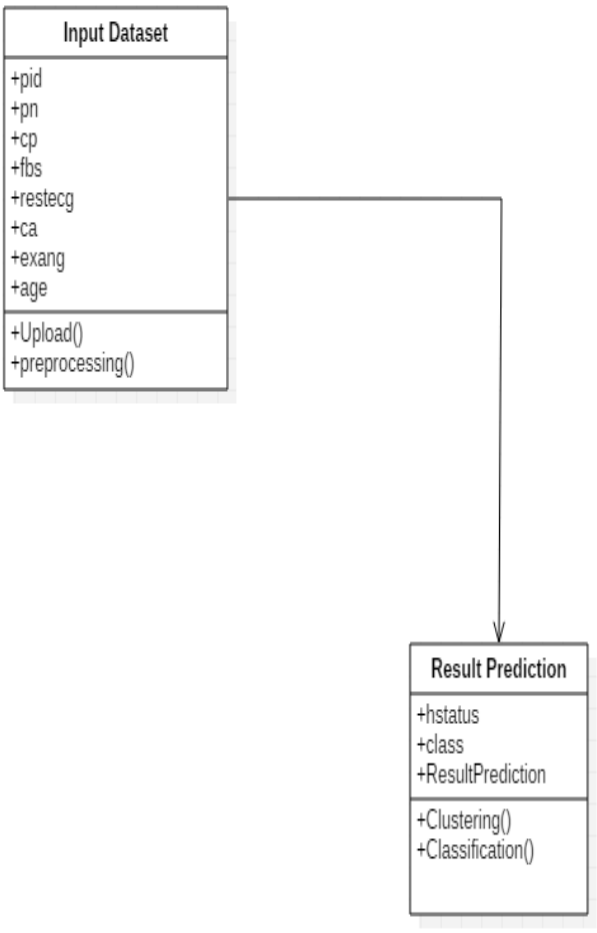
The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

USE CASE DIAGRAM

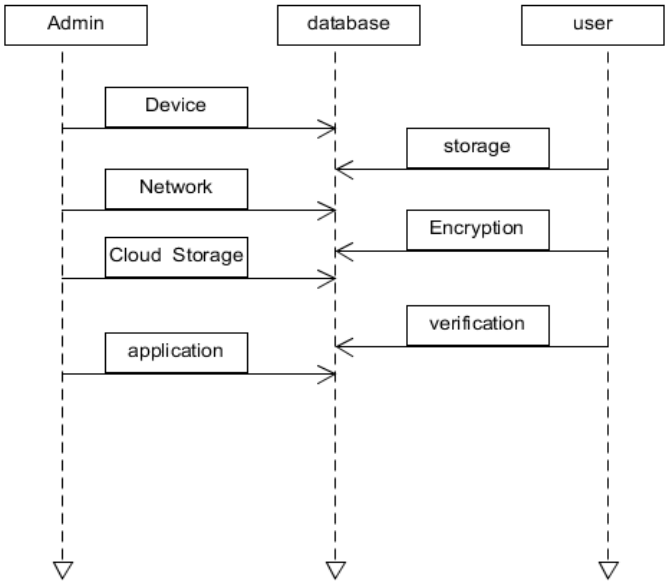
A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



CLASS DIAGRAM



SEQUENCE DIAGRAM



6 ALGORITHM:

6.1 SHA3-256 ALGORITHM:

SHA3-256 or Secure Hash Algorithm 3 is one of several cryptographic hash functions that takes input and produces a 256-bit (32-byte) hash value. This message digest is usually then rendered as a hexadecimal number which is 64 digits long.

SHA3-256 is most often used to verify that a file has been unaltered. This is done by producing a checksum before the file has been transmitted, and then again once it reaches its destination .

6.2 WHEN WAS SHA3 256 RELEASED?

SHA3-256 is part of SHA-3 (Secure Hash Algorithm 3) released by National Institute of Standards and Technology (NIST) on Aug 2015.

6.3 WHAT IS HASHING?

Hashing is the process of scrambling raw information to the extent that it cannot reproduce it back to its original form. It takes a piece of information and passes it through a function that performs mathematical operations on the plaintext. This function is called the hash function, and the output is called the hash value/digest.

As seen from the above image, the hash function is responsible for converting the plaintext to its respective hash digest. They are designed to be irreversible, which means your digest should not provide you with the original plaintext by any means necessary. Hash functions also provide the same output value if the input remains unchanged, irrespective of the number of iterations.

6.4 WHAT HAPPENS WHEN SHA3-256 HASH FUNCTION GENERATES

SHA3-256 hash function generator generates a SHA3-256 hash which can be used as secure 64 Hexadecimal password or used as Key to protect important data such as Insurance Company's data, financial market data, Personal Information and much. more.

It will generate 64 characters of SHA3-256 hash string and it cannot be reversible.

CONCLUSION

To rank the security of home consumer devices. An IoT lens based on the current state-of-the-art research in security of smart home devices was used to propose a novel methodology.

The derived AHP model also showed the importance of various security factors in current home consumer devices in an explicit and quantitative manner. In addition to ranking consumer devices, the AHP model can also be used to inform future research because it incorporates empirical security studies as well. In this methodology can be mostly automated and applied whenever the underlying information changes.

FUTURE WORK

The primary weak point in the future. In this case, the proposed methodology can be used to simply recalculate the priorities. Finally, it would also be interesting to compare these device rankings with those based on an AHP built using expert opinions. However, the advantage of the proposed methodology over an expert-based approach is that the methodology can be mostly automated and applied whenever the underlying information changes.

REFERENCE

[1] M. Inoue, K. Uemura, Y. Minagawa, M. Esaki, and Y. Honda, ‘‘A home automation system,’’ IEEE Trans. Consum. Electron., vol. CE-31, no. 3, pp. 516–527, Aug. 1985, doi: 10.1109/TCE.1985.289966.

[2] D. Kumar. All Things Considered: An Analysis of IoT Devices on Home Networks. Accessed: Oct. 1, 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/kumardeepak

[3] D. Pishva and K. Takeda, ‘‘A product based security model for smart home appliances,’’ in Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol., Lexington, KY, USA, 2006, pp. 234–242, doi: 10.1109/CCST.2006.313456.

[4] C. Lee, L. Zappaterra, K. Choi, and H. A. Choi, ‘‘Securing smart home: Technologies, security challenges, and security requirements,’’ in Proc. Conf. Commun. Netw. Secur., 2014, pp. 67–72, doi: 10.1109/CNS.2014.6997467.

5] (2019). Avast Smart Home Report 2019. Accessed: Jan. 15, 2022. [Online]. Available: https://press.avast.com/press-kits/avast-smart-homereport-2019

[6] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, ‘‘Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach,’’ in Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI), Beijing, China, Jul. 2017, pp. 179–181, doi: 10.1109/ISI.2017.8004904.

[7] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, ‘‘An experimental study of security and privacy risks with emerging household appliances,’’ in Proc. IEEE Conf. Commu. Netw. Secur., San Francisco, CA, USA, Oct. 2014, pp. 79–84, doi: 10.1109/CNS.2014.6997469.

[8] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, ‘‘Security vulnerabilities of Internet of Things: A case study of the smart plug system,’’ IEEE Internet Things J., vol. 4, no. 6, pp. 1899–1909, Dec. 2017, doi: 10.1109/JIOT.2017.2707465.

[9] Z. Celik, E. Fernandes, E. Pauley, and G. Tan, ‘‘Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities,’’ ACM Comput. Surv., vol. 52, no. 4, pp. 1–30, 2019, doi: 10.1145/3333501.

[10] H. Liu, C. Li, X. Jin, J. Li, Y. Zhang, and D. Gu, ‘‘Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices,’’ in Proc. Workshop Internet Things Secur. Privacy, New York, NY, USA, Nov. 2017, pp. 13–18, doi: 10.1145/3139937.3139948.

[11] S. Mare, L. Girvin, F. Roesner, and T. Kohno, ‘‘Consumer smart homes: Where we are and where we need to go,’’ in Proc. 20th Int. Workshop Mobile Compu, Sys. Appl., Santa Cruz, CA, USA, Feb. 2019, pp. 117–122, doi: 10.1145/3301293.3302371.

[12] J. M. Batalla, A. Vasilakos, and M. Gajewski, ‘‘Secure smart homes: Opportunities and challenges,’’ ACM Comput. Surv., vol. 50, no. 5, pp. 1–32, 2017, doi: 10.1145/3122816.

[13] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, ‘‘Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures,’’ IEEE Wireless Commun., vol. 25, no. 6, pp. 53–59, Dec. 2018, doi: 10.1109/MWC.2017.1800100.

[14] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, ‘‘Smart meter data privacy: A survey,’’ IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017, doi: 10.1109/COMST.2017.2720195. [15] N. Komninos, E. Philippou, and A. Pitsillides, ‘‘Survey in smart grid and smart home security: Issues, challenges and countermeasures,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014, doi: 10.1109/COMST.2014.2320093.

[16] S. D. Johnson, J. M. Blythe, M. Manning, and G. T. W. Wong, ‘‘The impact of IoT security labelling on consumer product choice and willingness to pay,’’ PLoS ONE, vol. 15, no. 1, pp. 33–48, Jan. 2020, doi: 10.1371/journal.pone.0227800.

[17] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, ‘‘User perceptions of smart home IoT privacy,’’ in Proc. ACM Hum. Comput. Interact., vol. 2, pp. 1–20, Nov. 2018, doi: 10.1145/3274469.

[18] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, ‘‘Ask the experts: What should be on an IoT privacy and security label?’’ in Proc. IEEE Symp. Secur. Priv. (SP), San Francisco, CA, USA, May 2020, pp. 447–464, doi: 10.1109/SP40000.2020.00043.

[19] J. M. Blythe and S. D. Johnson, ‘‘The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices,’’ in Proc. Living Internet Things, Cybersecurity, London, U.K., 2018, pp. 4–7, doi: 10.1049/cp.2018.0004.

[20] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, ‘‘SoK: Security evaluation of home-based IoT deployments,’’ in Proc. IEEE Symp. Secur. Priv., vol. 1, San Francisco, CA, USA, May 20-22, 2019, pp. 1362–1380, doi: 10.1109/SP.2019.00013.

[21] A. Mardani, A. Jusoh, K. MD Nor, Z. Khalifah, N. Zakwan, and A. Valipour, ‘‘Multiple criteria decision-making techniques and their applications—A review of the literature from 2000 to 2014,’’ Econ. Res. EkonomskaIstraivanja, vol. 28, no. 1, pp. 516–571, Jan. 2015, doi: 10.1080/1331677X.2015.1075139.

[22] T. L. Saaty, ‘‘Decision making with the analytic hierarchy process,’’ Int. J. Serv. Sci., vol. 1, no. 1, pp. 1–16, 2008. [Online]. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJSSCI.2008. 017590, doi: 10.1504/IJSSCI.2008.017590.

[23] T. L. Saaty and L. G. Vargas, ‘‘How to make a decision,’’ in Models, Methods, Concepts & Applications

of the Analytic Hierarchy Process. Boston, MA, USA: Springer, 2012, pp. 1–21.

[24] I. Syamsuddin and J. Hwang, ‘‘the application of AHP model to guide decision makers: A case study of E-banking security,’’ in Proc. 4th Int. Conf. Comput. Sci. Converg. Inf. Technol., Nov. 2009, pp. 1469–1473, doi: 10.1109/ICCIT.2009.251.

[25] D. Maáek, I. Magdaleni, and N. Reáep, ‘‘A systematic literature review on the application of multicriteria decision making methods for information security risk assessment,’’ Int. J. Saf. Secur. Eng., vol. 10, no. 2, pp. 161–174, Apr. 2020, doi: 10.18280/ijsse.100202.

[26] S. Gupta Bhol, J. Mohanty, and P. Kumar Pattnaik, ‘‘Taxonomy of cyber security metrics to measure strength of cyber security,’’ Mater. Today, Proc., Jun. 2021. [Online]. Available: https://www-sciencedirectcom.aus.idm.oclc.org/science/article/pii/S2214785321046009? via%3Dihub, doi: 10.1016/j.matpr.2021.06.228.

[27] X. Zhao, H. Xu, T. Wang, X. Jiang, and J. Zhao, ‘‘Research on multidimensional system security assessment based on AHP and gray correlation,’’ in Proc. Trusted Comput. Inf. Secur., Singapore, 2020, pp. 177–192, doi: 10.1007/978-981-15-3418-8_13.

[28] F. H. Sohime, R. Ramli, F. A. Rahim, and A. A. Bakar, ‘‘Exploration study of skillsets needed in cyber security field,’’ in Proc. 8th Int. Conf. Inf. Technol. Multimedia (ICIMU), Aug. 2020, pp. 68–72, doi: 10.1109/ICIMU49871.2020.9243448.

[29] J. Zaburko and J. Szuláyk-Cieplak, ‘‘Information security risk assessment using the AHP method,’’ IOP Conf. Ser., Mater. Sci. Eng., vol. 710, no. 1, Dec. 2019, Art. no. 012036, doi: 10.1088/1757-899X/710/1/012036.

[30] L. D. Bodin, L. A. Gordon, and M. P. Loeb, ‘‘Evaluating information security investments using the analytic hierarchy process,’’ Commun. ACM, vol. 48, no. 2, pp. 78–83, Feb. 2005, doi: 10.1145/1042091.1042094.

[31] H. Wang, Z. Sun, H. Wang, and Z. Sun, ‘‘Research on multi decision making security performance of IoT identity resolution server based on AHP,’’ Math. Biosci. Eng., vol. 18, no. 4, pp. 3977–3992, 2021, doi: 10.3934/mbe.2021199.