Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Cyber Security in Data Breaches

Ayed Aldossary [1] ،Talal Algirim [1] Ibrahim Almubarak, [1] Khalid Almuhish[1]

[1]*Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

ARTICLE INFO

Article History

Received: 01-11-2024
Revised: 30-11-2024
Accepted: 08-12-2024
Published: 09-12-2024

Academic Editor:

Prof. Youakim Badr

Vol.2024, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2024.1.3

ABSTRACT

In today's increasingly digital world, cyber-attacks have emerged as one of the most pressing threats to individuals, organizations, and national infrastructure. The consequences of such attacks are far-reaching, including financial losses, disruptions to daily operations, exposure of sensitive data, and even risks to public safety and national security. As cyber threats grow in frequency and sophistication, the ability to detect and prevent them becomes more critical. Notably, social media has shown potential as a tool for early detection of cyber incidents, with users acting as real-time social sensors. However, leveraging open-source indicators from social media remains a complex challenge due to the unstructured nature of the data and potential misinformation. Furthermore, as the integration of emerging technologies becomes central to business efficiency and innovation, the corresponding increase in cyber vulnerabilities poses significant risks. Data breaches—whether intentional or accidental—represent a persistent danger to organizations of all sizes, often involving the unauthorized exposure of confidential personal and corporate information. To address these threats, this paper explores technical cybersecurity practices such as the deployment of firewalls, malware protection, intrusion detection systems (IDS), and other defense mechanisms that help eliminate vulnerabilities and strengthen digital resilience. The paper emphasizes the importance of a proactive, multi-layered cybersecurity strategy to safeguard data and ensure secure, trustworthy digital environments.

Keywords: Cyber-attacks; Intrusion Detection Systems (IDSs); Firewalls, Malware.

How to cite the article
Aldossary, A., Algirim, T., Almubarak, I., & Almuhish, K. (2024). Cyber Security in Data Breaches. Journal of Cyber Security and Risk Auditing, 2024(1), 14–22. https://doi.org/10.63180/jcsra.thestap.2024.1.3

**Corresponding author. Email: 216010826.student@kfu.edu.sa*

1. Introduction

1st Today's widespread incidences of cyber-attacks, each more audacious than earlier ones, makes them perhaps the primary threat faced by individuals, organizations, and nations alike [1] . Consequences and implications of cyber-attacks include monetary losses, threats to critical infrastructure and national security, disruptions to daily life, a potential to cause loss of life and physical property, and data leaks exposing sensitive personal information about users and their activities. It has been well argued that, because news about an organization's compromise sometimes originates outside the organization, one could use open-source indicators as indicators of a cyber-attack [2]. Social media, in particular, turns users into social sensors empowering them to participate in an online ecosystem of event detection for happenings such as disease outbreaks, civil unrest , and earthquakes . At the same time, it is non-trivial to harness social media to identify cyber-attacks [3].

The industry of it is expected that in the future will be marked with multiple technologies and it has a very important role for the efficiency of the company's expectations, unfortunately there will be threats that will come to the security of the companies [4]. Some technologies will be discussed to prevent these threats against attackers, by providing the technology needed it can develop a strong and secure place for the data in companies and prevent attacks and ensuring and guarantying a safe and secure environment for the data [5].

A data breach is an incident in which confidential and sensitive, or any protected data is illegally accessed or disclosed without permission [6]. This issue can involve theft or loss of sensitive information such as social security number and password, data breach is often associated with crucial information such as credit card numbers and CVV code, social security numbers, medical history, and insurance setup. Besides, data breaches can also target large corporations which aim to obtain customer list, product source code, trade secrets, and payment information. A data breach does not consider the size of the company as both small and established institutions have reported cases of data breaches. Breach of information represents a permanent threat to any organization. Data breach can be intentional or accidental. Creating defense or defending computers, networks and servers and data against malicious attack. Eliminating vulnerable points that can be used by attackers to gain access into the system. The technical cyber security practices are those that lean towards the technical foundation of an organization. Such as installing firewall, installing malware, or adopting an IDS [7].

As cyber threats grow in frequency and sophistication, the ability to detect and prevent them becomes more critical. Notably, social media has shown potential as a tool for early detection of cyber incidents, with users acting as real-time social sensors. However, leveraging open-source indicators from social media remains a complex challenge due to the unstructured nature of the data and potential misinformation. Furthermore, as the integration of emerging technologies becomes central to business efficiency and innovation, the corresponding increase in cyber vulnerabilities poses significant risks. Data breaches—whether intentional or accidental—represent a persistent danger to organizations of all sizes, often involving the unauthorized exposure of confidential personal and corporate information. To address these threats, this paper explores technical cybersecurity practices such as the deployment of firewalls, malware protection, intrusion detection systems (IDS), and other defense mechanisms that help eliminate vulnerabilities and strengthen digital resilience. The paper emphasizes the importance of a proactive, multi-layered cybersecurity strategy to safeguard data and ensure secure, trustworthy digital environments.

2. Types of data breaches

It involves a criminal attacker encrypting files and blackmails target organization or victim into paying money in exchange for the decryption key. The attackers threaten to destroy critical data if the victim or affected organizations fail to comply with extortion demands. The data breaches types will be as follows:

2.1 Denial of service (DoS attack)

A denial-of-service attack (DoS attack) is a cyber-attack it intends to make machine unavailable temporarily or indefinitely and disrupts the host connected to the internet [8].

2.2 Phishing

it is a type of social engineering attack often used when an attacker lore victim to a message from text or by email and steal the victim data like credit card, names, and passwords [9].

2.3 Malware

A malware attack is a common cyberattack where malware it establishes viruses that impact and harm users to execute unauthorized actions on the system [10].

2.4 Cybersecurity measures:

Management of data breaches involves a combination of various measures which can be categorized into; technical, organizational, policies and standards. The cybersecurity measures that can be used to prevent data breaches in an organization [11]. These measures are presented below.

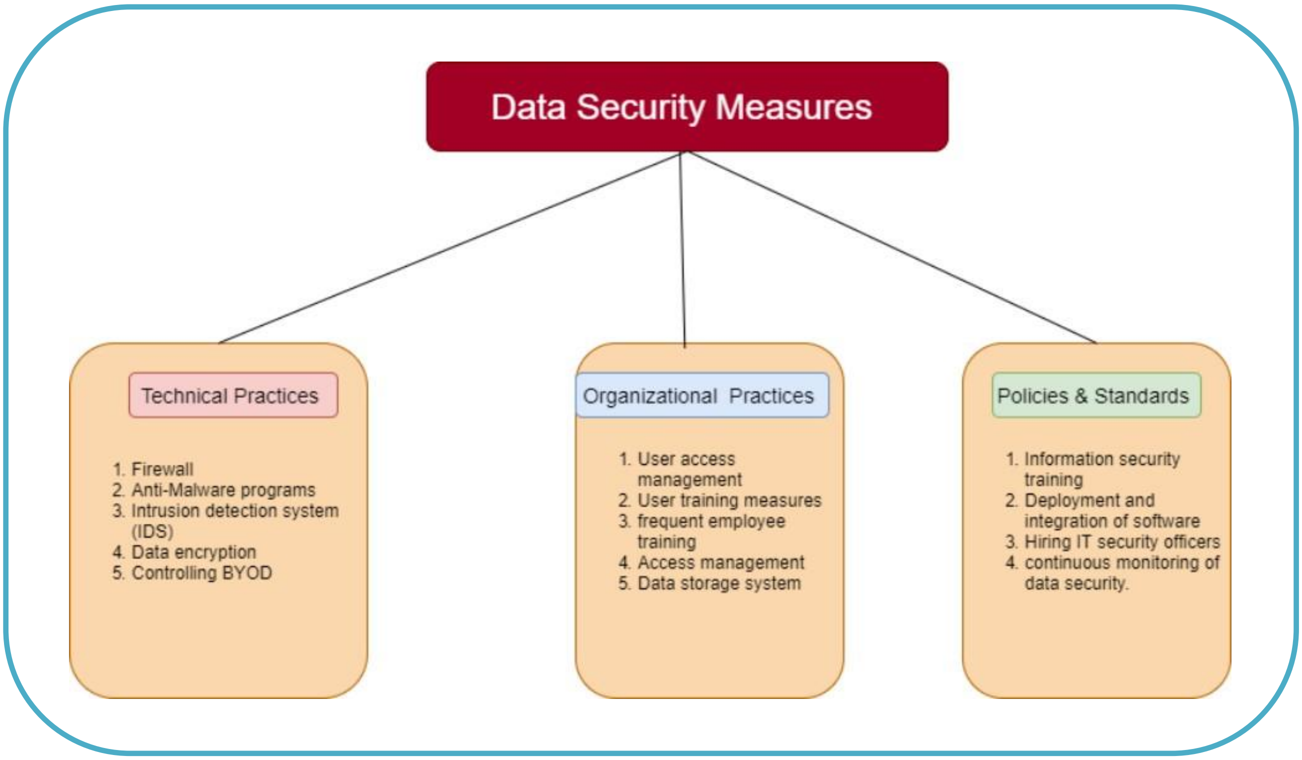

Data Security Measures
Technical Practices
1. Firewall
2. Anti-Malware programs
3. Intrusion detection system (IDS)
4. Data encryption
5. Controlling BYOD
Organizational Practices
1. User access management
2. User training measures
3. frequent employee training
4. Access management
5. Data storage system
Policies & Standards
1. Information security training
2. Deployment and integration of software
3. Hiring IT security officers
4. continuous monitoring of data security.

Figure 1. Data Security Measures [11]

2.5 Cases studies on data breaches

2.5.1 Adobe

In October 2013, an incident happened with the adobe application that affected 153 M user records. The security blogger Brian Krebs reported that hacker had stolen about 3M encrypted passwords of 38M active users such as credit card information and login data of the users. Later, the blogger has an estimation to include IDs and passwords for 38M users and more than 150M usernames and passwords taken from the application, this made adobe to settle claims of violated customers to pay 1.1M in legal fees [12].

2.5.2 EBay

In 2013-2014, yahoo reported that 3 Billion user accounts impact, one of the biggest data breaches in history when yahoo announced about the breach. Yahoo claimed most of the impacted passwords which they believed about compromising names, emails, dates of birth and telephone numbers. Later in December 2016, yahoo encountered another attacker form 2013 that he spotted the users information of 1 Billion accounts. Verizon has acquired yahoo and paid about 4.48 Billion for its core internet business while the breach stolen an estimation about 350M off the value of the company [13].

3. Methodology

In traditional information extraction (IE), a large corpus of text must first be annotated to train extractors for event triggers, defined as main keywords indicating an event occurrence [14]. However, in our scenario using online social media, a manually annotated label set is impractical due to the huge volume of online media and the generally noisy characteristics of the text. In this section, we propose a novel method to automatically mine query templates over which the event tracking is performed.

3.1 Target Domain Generation

In this subsection, we propose the method of target domain generation, which serves as the source of social indicators for the detection of ongoing cyber-attack events. Given a query and a collection of tweets D, the typical way to retrieve query-related documentation is based on a bag of words model which comes with its attendant disadvantages.

3.2 Dynamic Typed Query Expansion

In this subsection, we propose a way to dynamically mine an expanded query given a small collect of seed query, as shown in Table 1. By providing a small set of seed queries (unigrams), [14] proposed a dynamic query expansion (DQE) method which is able to iteratively expand the seed query set from currently selected target tweet subspace until convergence. Looking beyond the simple unigrams-based expansion, by introducing dependency-based tree structure extraction, we build a dynamic expanded query generation model for the cyber-attack detection task.

3.3 Event Extraction

Given an expanded query set Q, we extract Qs | qi □ qj | qi , qj ∈ Qs . For example, consider the surface string representations of a set of expanded queries Q as then Qs will be .Each exemplar query qe is then annotated to a cyber-attack type.
Sim = e j.

For the complete event representation date information is extracted based on the time interval chosen for DQE; for example, in our experiments we run DQE on a daily aggregated collection of tweets. Let D denote the tweet space corresponding to a sub collection Di , let D+ denote the target tweet subspace , and let D− = D − D+ denote the rest of the tweets in the considered tweet space. Definition 1. Different from n-grams, terms contained in a typed dependency query share both syntactic and semantic relationships. Mathematically, a typed dependency query is formulated as a tree structure G = {V , E}, where node v ∈ V can be either a unigram, user mention, or a hashtag and ∈ E represents a syntactic relation between two nodes [15], [16],[17].

4. Evaluation

4.1 Evaluation Setup

Dataset and Gold Standard Report. We evaluate the proposed method on a large stream of tweets from GNIP's decahose (10% sample) collected from August 2014 through October, 2016. The total raw volume of our Twitter dataset across these 27 months is 5,146,666,178 (after removing all retweets). Then, from this raw volume we create 2 subset collections.

4.2 Measuring Performance

These results shows that with only a small set of seed query templates , our approach can reach around 80% of precision for data breach and DDoS events. Careful manual analysis indicates that we actually detected new account hijacking events that are not covered by the GSR. The manual validation results for data breach and DDoS events are shown in Table 3. We also detected new events that are not covered by GSR for these two types.

We capture 12 separate events of DDoS attacks including four in last week of August 2014, starting with the first on August 24th. Further in 2015, more ensuing attacks are captured one highlighted by the data breach of their movie production house, on December 12th and then a massively crippling targeted, DDoS attack on their PlayStation network in late December, 2015. Another noteworthy case of DDoS attacks in 2016, is the multiple distributed denial-of-service attack on DNS provider «Dyn» from October 21st through 31st in 2016 that almost caused a worldwide internet outage. 4 which clearly characterizes the nature of these DDoS attacks where the hackers turned a large number of internet-connected devices around the world into botnets executing a distributed attack.

Specific techniques range from classifying malicious network flows to anomaly detection in graphs to detect malicious servers and connections. More recently, researchers seek to move ahead to predict cyber-attacks before they happened for early notifications. In recent years, online media such as blogs and social networks become another promising data source of security intelligence. Most existing work focuses on technology blogs and tweets from security professionals to extract useful information. Building text mining tools to extract key attack identifiers from security tech blogs .leverage Twitter data to estimate the level of interest in existing CVE vulnerabilities, and predict their chance of being exploited in practice. Our work differs from existing literature since we focus on crowdsourced data from the much broader user populations who are likely the victims of security attacks. The most related work to ours is which uses weakly supervised learning to detect security related tweets.

4.3 Cyber-Assets at Risk (CAR)

Data breach incidents have been fast becoming a vital instrument in cyber-security risk assessment.one of the most important point to keep the reputation of any company or organization is the security of data. By securing company's data will avoid financial fees or litigations. Data breach can cost the company a hundreds of million dollars, which can harshly impact organization's financial health. For that reason, decision-makers must understand the impact and damages of data breach on the organization and invest in cyber-security.

4.4 Information categorization

This study categorizes two types of information/data that can be breached as listed:

personally, identifiable information (PII): as what the department of homeland security defines the PII as (DHS, 2017): "any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department."

Sensitive PII (SPII): is defined as "personally identifiable information which, if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual."(DHS, 2017).

Table 1. An example of PII

PII
Name
Account name/ user ID
Password
Email
Address

Telephone number
Education credentials/certificates
Date/place of birth
Vehicle title number

Table 2. An example of SPII

SPII
Social security numbers
Medical history
Credit/ debit card numbers
Driver’s license numbers
Bank account numbers
Passport numbers
Alien registration numbers
Biometric identifiers

What will benefit the hacker to steal PII? The main reason is to make money by duplicating credit card or printing passports. After that process hackers’ sales this information in the dark web. Other than that, some hackers steal it out of fun or challenge. The study stated that PII breach could be done by intentional or unintentional leak. Finance and healthcare industries are the most targeted to the malicious activities. The most stolen data from the organizations are credit cards and medical information.

Table 3. Healthcare law

Civil Sanctions	Criminal sanctions
As a consequence of failure to acknowledgment, fine cost ($100 - 25,000). If it is repeated it will start it will cost ($50,000 - 1, 5 million).	For individuals who get or reveal individually identifiable health information intentionally there will be a fine which cost ($50,000) + imprisonment for up to 1 year.
Due to reasonable cause and not due to willful neglect. Fine Cost ($1000 - 100,000). Also, if it is repeated the fine will cost ($50,00 - 1,5 million)	For crimes committed under pretenses there will be a fine cost ($100,000)+ imprisonment for up to 5 years.
Due to intentional neglect, with violation corrected within the required time. Costs ($10,000 – 250,). If repeated the cost will be ($ 50,000 – 1,5 million)	For the use of individually identifiable health information for commercial advantage there will be a fine cost ($250,000)+ imprisonment for up to 10 years.
Due to intentional neglect and not corrected. Fine cost ($50,000 – 1,00,00)	\\

With the influence of COVID-19 in our daily life, and cyber security becomes more related than before. The way to communicate has been moved to another level which is remote information technology, and that opened a new gate of cyber incidents and attacks. The most popular attacks that exist today are phishing schemes and ransomware. Moreover, applications of remote working, such as collaboration and file sharing tools, devices that connect to the network, traffic of higher email, end to end solutions of cloud. All of these applications may lead to data beeches.

In the pandemic, most of the organizations switched to telecommuting. With that movement, all the transactions will be under threat, if the companies will not have any idea about their valuable data, and how can be compromised by the attackers. During these months, most the security companies have been educates the community about the cyber security hazards. The pandemic forced the workforce to move out of corporate premises and students out of their schools into virtual environments in which that cause the systems to become more vulnerable due to less awareness. Remote access to companies' system and their data is critical for this type of work to function. While the companies ask their employees to work from homes, it will increase the vulnerability of IT system infrastructures. The level of protection is different from employee to another. While the employee uses his personal device to access the server remotely, as well as his private wireless connection, these things considered as potential entry points for the cyber criminals. In addition, when the employee is a phishing victim in which that the company is vulnerable, and their data cannot be reachable due to cyber-attack and that lead us to data breaches.

Common types of Data breaches: While the organizations lose or accidentally disclose their data, it can be through hacking or negligence. The first type is ransomware, this type is malicious software in which that can encrypts the files, restore data, and block the victim from accessing his own data. Second type is malware, basically, any software that designed to cause harm damage to the target computer. There are several types of malware which are Worm, Trojan horse, and Ransomware. The third type is phishing, this type is known fraudulent attempt to get sensitive information, or data from the victim.

5. Conclusion

We have demonstrated an unsupervised approach to extract and encode cyber-attacks reported and discussed in social media. Given the widespread prevalence of cyber- attacks, tools such as presented here are crucial to providing situational awareness on an ongoing basis. Future work is aimed at broadening the class of attacks that the system is geared to as well as at modeling sequential dependencies in cyber-attacks. However, leveraging open-source indicators from social media remains a complex challenge due to the unstructured nature of the data and potential misinformation. Furthermore, as the integration of emerging technologies becomes central to business efficiency and innovation, the corresponding increase in cyber vulnerabilities poses significant risks. Data breaches—whether intentional or accidental—represent a persistent danger to organizations of all sizes, often involving the unauthorized exposure of confidential personal and corporate information. To address these threats, this paper explores technical cybersecurity practices such as the deployment of firewalls, malware protection, intrusion detection systems (IDS), and other defense mechanisms that help eliminate vulnerabilities and strengthen digital resilience. The paper emphasizes the importance of a proactive, multi-layered cybersecurity strategy to safeguard data and ensure secure, trustworthy digital environments.

Corresponding author

Ayed Aldossary
216010826.student@kfu.edu.sa

Acknowledgements
NA

Funding
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia.

Contributions
A.A; T.A; I.A; K.A; Conceptualization, A.A; T.A; I.A; K.A; Investigation, A.A; T.A; I.A; K.A; Writing (Original Draft), A.A; T.A; I.A; K.A; Writing (Review and Editing) Supervision, A.A; T.A; I.A; K.A; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

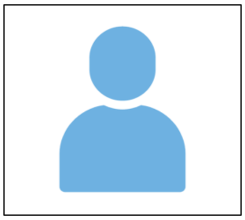
Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

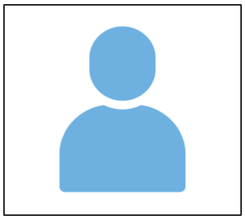
References

[1] Mu, X., & Antwi-Afari, M. F. (2024). The applications of Internet of Things (IoT) in industrial management: A science mapping review. *International Journal of Production Research, 62*(5), 1928–1952.
[2] Al-Mekhlafi, Z. G., Al-Janabi, H. D. K., Khalil, A., Al-Shareeda, M. A., Mohammed, B. A., Alsadhan, A. A., Alayba, A. M., Saleh, A. M. S., Al-Reshidi, H. A., & Almekhlafi, K. (2024). Lattice-based cryptography and fog computing-based efficient anonymous authentication scheme for 5G-assisted vehicular communications. *IEEE Access.*
[3] Kalpana, M. M. (2025). Survey and analysis of home automation system encompassing embedded systems, the Internet of Things (IoT) and AI algorithms. *Vidhyayana – An International Multidisciplinary Peer-Reviewed E-Journal, 10*(SI4).
[4] Nassereddine, M., & Khang, A. (2024). Applications of Internet of Things (IoT) in smart cities. In *Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy* (pp. 109–136). CRC Press.
[5] Al-Shareeda, M. M. A., Anbar, M., Alazzawi, M. A., Manickam, S., & Hasbullah, I. H. (2020). Security schemes based conditional privacy-preserving in vehicular ad hoc networks. *Indonesian Journal of Electrical Engineering and Computer Science, 21*(1).
[6] Santhikiran, B., Nagaraju, L., Sattar, S. A., Chandra, D. B., & Jayasankar, Y. (2023). Design and implementation of smart home system based on IoT and ESPRainmaker. *International Transactions on Electrical Engineering and Computer Science, 2*(2), 70–79.
[7] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A holistic analysis of Internet of Things (IoT) security: Principles, practices, and new perspectives. *Future Internet, 16*(2), 40.
[8] Al-Shareeda, M. A., Anbar, M., Manickam, S., Hasbullah, I. H., Abdullah, N., Hamdi, M. M., & Al-Hiti, A. S. (2020). NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs). *Applied Mathematics, 14*(6), 1–10.
[9] Uzoka, A., Cadet, E., & Ojukwu, P. U. (2024). The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications. *Comprehensive Research and Reviews in Science and Technology, 2*(02), 055–073.
[10] Al-Shareeda, M. A., Manickam, S., Saare, M. A., & Arjuman, N. C. (2023). Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network. *Indonesian Journal of Electrical Engineering and Computer Science, 29*, 518–526.
[11] Mustofa, A. A., Dagnew, Y. A., Gantela, P., & Idrisi, M. J. (2023). SECHA: A smart energy-efficient and cost-effective home automation system for developing countries. *Journal of Computer Networks and Communications, 2023*(1), 8571506.
[12] Aghenta, L. O., & Iqbal, T. (2019). Design and implementation of a low-cost, open source IoT-based SCADA system using ESP32 with OLED, ThingsBoard and MQTT protocol. *IMS Electronics and Electrical Engineering, 4*(1), 57–86.
[13] Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2022). Intelligent drone-based IoT technology for smart agriculture system. In *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)* (pp. 41–45). IEEE.
[14] Siswanto, A., Efendi, A., & Kadir, E. A. (2023). Biometric face authentication system for secure smart office environments. *Indonesian Journal of Electrical Engineering and Computer Science, 32*(2), 1134–1141.
[15] Irugalbandara, I. C., Naseem, A., Perera, M., & Logeeshan, V. (2022). HOMEIO: Offline smart home automation system with automatic speech recognition and household power usage tracking. In *2022 IEEE World AI IoT Congress (AIIoT)* (pp. 571–577). IEEE.
[16] Litayem, N. (2024). Scalable smart home management with ESP32-S3: A low-cost solution for accessible home automation. In *2024 International Conference on Computer and Applications (ICCA)* (pp. 1–7). IEEE.
[17] Jion, M. S. A., & Ahmad, M. (2024). A smart and secured office system using IoT. In *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)* (pp. 1–6). IEEE.

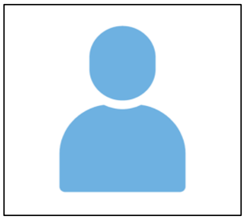
Biographies



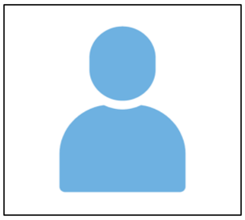
Ayed Aldossary, Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia. 216010826.student@kfu.edu.sa



Talal Algirim, Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia



Ibrahim Almubarak, Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia



Khalid Almuhish, Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia