The Positive Impact of Intelligent Agent in IoT Data Security and Privacy

[1]Hafsa Tariq, [2]M. Junaid Arshad

[1,2]Department of Computer Science, University of Engineering and Technology, Lahore-Pakistan

***Abstract*—The paper provides an overview of an article discussing the importance of data security in IoT and how it is critical for protecting all other aspects of IoT, including privacy. The paper highlights the need for data security and privacy preserving methods in IoT due to the increasing number of IoT devices and potential cyber threats. It describes various techniques, including machine learning algorithms, blockchain, encryption, and access control, to secure IoT data and reduce vulnerabilities and data breaches. The paper also discusses the challenges related to data security in IoT concerning intelligent agents, such as authentication and authorization, encryption, data privacy, device security, and interoperability. The paper proposes a combination of technological solutions, best practices, and compliance with privacy regulations to address these challenges. It also discusses advanced technologies and approaches, such as blockchain technology and machine learning-based anomaly detection, to ensure the integrity and security of IoT data. Finally, the paper emphasizes the positive impacts of data security and privacy in IoT, including protection of sensitive data, building trust, compliance with regulations, prevention of cyberattacks, and improved operational efficiency.**

***Keywords*– Intelligent Agent, Data Security, Impact, Encryption, Block chain, Privacy Protection, Unauthorized User and Authentication**

I. INTRODUCTION

IN the past recent years, when their internet-based era, technologies, and new applications faced securities issues. The devices that are connected to the internet may have a high-risk factor of cyber threats [1]. There are no specific protocols to protect the data from mitigating attackers and breaches. Attacks are of a different kind including phishing, DDoS, spamming, spoofing, malware, and hacking [2]. According to roughly an estimated 127 new IoT devices connected every second. The number of devices connected via IoT will be reached 25 million by 2025, which is the third fold increase from 2017.

An intelligent agent is one of the fields of artificial intelligence. Nowadays every machine is based on an intelligence agent and when it is connected to the internet, it becomes an IoT device. IoT gives the concept of a higher level of integrity, availability, confidentiality, accessibility, and scalability to the whole world [3]. If we interlink with the intelligent agent, then there are two types of impact positive and negative in IoT data.

The purpose of this paper is to describe the positive impact of an intelligence agent in IoT data security and protection [4]. There are several kinds of positive impacts of intelligence agents including data security, real-time analysis, personalized data access, risk management, and authorized data protection.

Data security is one of the basic needs of every IoT-based user, every user wants to protect their data from attackers, threats, and viruses. This paper describes the data security impact of an intelligent agent on IoT data [5]. Although data security nowadays in the digital world includes cyber-attacks, insider threats, compliance, complexity, and data volume [6]. All these challenges need to be addressed, so that the devices connected via IoT work smoothly with proper protection.

IoT and AI both devices rely on wireless communication and are connected using wireless protocols. IoT devices collect user data often without giving intimation to the users [7]. This may cause vulnerabilities to the data and consider to be theft data. The collection and processing of data by IoT devices can raise privacy concerns [8]. There is a need to develop privacy preserving methods that allow for the collection and processing of data without compromising user privacy.

The overall conclusion of this paper is to provide the most recent data security techniques and methods that provide secure communication and data protection from threats, attacks, and viruses [9], [10]. Cover all the recent work that has already been done to save IoT-based data.

II. LITERATURE REVIEW

With the increase in IoT devices, the risk factor also increases. According to the research different methods and techniques are imposed onto the different scenarios to protect the data and secure it from attackers.

Machine learning algorithms are also used to protect the data and secure it from hackers [11]. The decision tree model algorithm is one of those, that is used for the protection of data and to reduce vulnerabilities and data breaches.

Blockchain is a new domain of cryptography that is used to secure data in IoT [12]. Data is secured into a different block; an attacker needs to identify the current authentic block which is quite difficult. With blockchain techniques, Tylor based BCCO method is used for the protection of data.

Blockchain is a decentralized distributed database, all the data is stored in it and arranged into chronological order and combine with the help of a chain [13]. The advanced technique of cryptography to secure the data, using a different algorithm to protect the vehicular data like elliptic curve cryptosystem, bilinear maps, and batch verification.

Encryption is another technique used in data security for the protection of data [14]. Everything nowadays is stored on the cloud platform which also helps to reduce memory and spatial factor. The method used for this purpose is a cloud platform based on database encryption to protect the security factor of data.

Data security is also done by using the inner product encryption (IPE) mechanism with blockchain to get access control in IoT devices for protection [15]. This method used the four-part system initialization, data encryption and storage, user registration, and data access.

A blockchain-based access control (ABAC) scheme is another method to protect the data in IoT using the domain of blockchain [16]. A huge data list can be maintained using this approach and blockchain provides a trustable platform to maintain the data [17]. Blockchain can help to solve the single point of failure problem in the centralized access control scheme.

Blockchain provides security to bitcoin cryptocurrency using the code obfuscation and AES encryption method with watermarking [18]. because it uses the ciphertext with the properties of a homomorphic algorithm.

III. METHODOLOGY

We follow the mention below methodology points to get the accurate result for our review paper.

A) Research Question and Objective

- Impact of AI on IoT data?
- What are the techniques of data security?
- What is the positive impact of AI on data security?
- How data can be secure in IoT using AI technology?

The main motto of these questions is to get the best result to fulfill our requirement and get to know about the latest techniques used to protect the data security in IoT using AI and how its impact effect Ion IoT.

B) Search strategy

The search strategy used in this paper depends upon the internet as it is the best teacher to guide. Different keywords like machine learning, blockchain, encryption of data, data security and protection in IoT, and issue in IoT data privacy are used to find out the result. Although different research papers are gathered to extract useful information from it.

C) Study selection

We used the approach of the diagram and table of literature survey in which all the past search work has been clearly described in detail. Although the diagram is also added to elaborate the meaning of context. Along with it, describes the different attacks and their solutions with advantages.

D) Data extraction

Data in this paper was collected from different research papers. most highlighted points extracted from the paper. Google Scholar is the best source to extract useful data and the Sci-Hub website is used to download useful papers.

E) Limitation

Although there is no limitation in this paper as we are focusing on the positive impact. apart from limitations, we proposed a future direction in which we put our opinion to get a better result using some new techniques after analyzing the different attacks and techniques of data security.

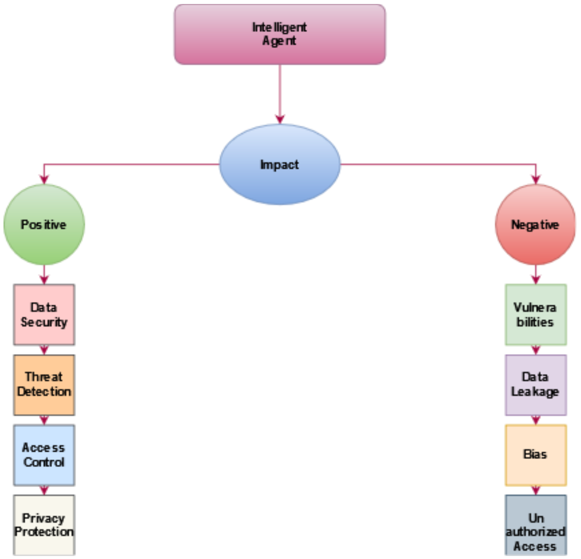

Fig. 1. Data Security with its Modules

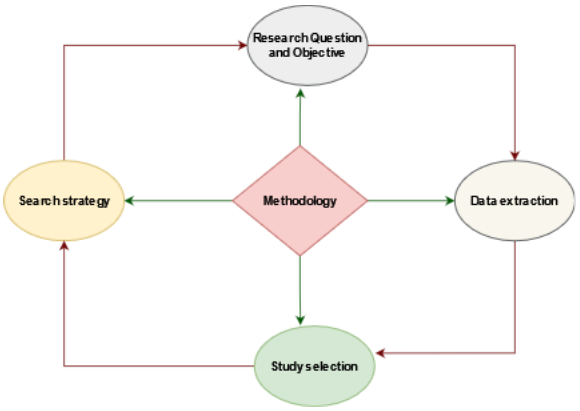

Fig. 2. Methodology used for Gathering the Data

IV. WHAT IS DATA SECURITY IN IOT?

Data security in IoT refers to the protection of data that is generated, processed, and transmitted by IoT devices and systems [19]. This data can include personal and sensitive information such as user IDs, passwords, location data, health data, and financial data.

TABLE I
EXISTING RESEARCH FOR IMPACT OF INTELLIGENT AGENT IN IOT DATA SECURITY AND PRIVACY

Authors	Year	Methodology	Technique	Algorithm
Jingfu Li	2020	Algorithm	Machine Learning	Decision Tree Model
Mohan Kumar Chandol	2023	Algorithm	Blockchain	Taylor bases BCCO
XiaoHong Zhang	2019	Vehicular Data	Blockchain	Elliptic Curve cryptosystem, Bilinear Maps
Xiaoqing Mai	2022	Cloud Platform Server	Encryption	Cloud Platform based Database Encryption
Pengchong Han	2023	Encryption	Blockchain	Inner Product Encryption (IPE)
Nannan Wu	2023	Cryptography	Blockchain	Blockchain based Access Control (ABAC)
Teng Huang	2023	Watermarking injection, bitcoin	Blockchain	Code Obfuscation, AES Encryption
Shashi Mishra	2022	Encryption	Blockchain	Blockchain
Faiqa Sajid	2022	Cryptography	Encryption	RSA Algorithm
Jyoti Moy Chatterjee	2019	Malicious Insider	Data Masking	Data Masking
Darpan Anand	2020	Encryption	Hashing	SHA-256
Ehia I Alzoubi	2020	True based routing mechanism	Routing and switching	Routing and switching Algorithm

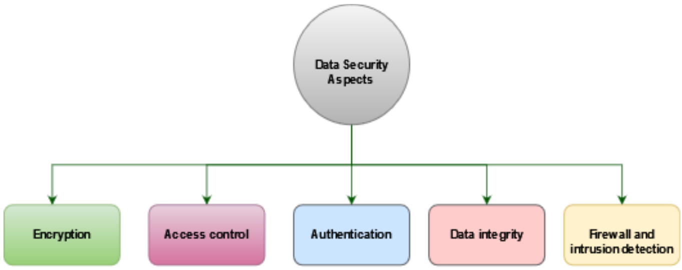

Fig. 3. Multiple Aspects used in IoT Data Security for Protection

Some key aspects of data security in IoT are as follows:

- Encryption
- Access control
- Authentication
- Data integrity
- Firewall and intrusion detection
- Regular updates and patches
- Secure software development

Overall data security in IoT is crucial to protect sensitive data and prevent unauthorized access to IoT systems.

V. WHY DATA SECURITY IS IMPORTANT AND WHY DO WE USE IT?

We use the data security for the following mention reasons:

- Protection of confidential information
- Compliance with regulation
- Prevention of data breaches
- Protection of intellectual property
- Trust and reputation

Data security measures help to prevent data breaches, minimize the impact of any breaches that do occur, and comply with data protection and regulation [20]. Strong data security measures can help build trust with customers and partners, which can lead to increased loyalty and revenue. Overall, data security in IoT is crucial in today’s digital age, where data is constantly being created, stored, and shared. It is essential to take proactive measures to secure data and ensure that it is protected from unauthorized access and misuse.

VI. TECHNIQUES USED IN DATA SECURITY

There are several techniques used in data security to protect sensitive information from unauthorized access, theft, and misuse person [21], [22]. Some of the most common techniques include:

A) Firewalls

It is an initial security layer in a system that is used to keep unauthorized sources away from the system access [23]. These are software and hardware-based security system that is used to monitor and filter the incoming and outgoing network traffic to prevent the data from unauthorized access:

- Application-level gateways
- Stateful inspection firewalls
- Basic packet-filtering firewall and soon.

B) Authentication and Unauthorized

Two processes ensure that only appropriate and authorized persons should get access to the enterprise data. Authentication involves the verification of the users that includes:

- Bio-metric
- Password or PIN

It also includes multi-factor authentication (MFA) to sign in with additional factors e.g., password or PIN, MFA, biometric, and soon. After the authentication process, authorization determines that the users have appropriate permission to get access to the data. After authorization user gains permission to edit, read and write by using different sources:

- Attribute-based access control
- Role-base access control

C) Data Encryption

This involves the use of a complex algorithm to convert plain text data into a secure, unreadable format that can only be decrypted with a key or password [24]. Encrypted data is meaningless for any attackers if attackers do not have the key or password:

- Asymmetric encryption
- Symmetric encryption

D) Data Masking

It is similar to encryption, but we use data masking to represent the fake data by replacing it with legitimate data [25][26]. Even if the criminal gets access to the data, then it can't make sense what they stole. This method is used in software testing or user training e.g.,

- Tokenization
- Data generalization
- Data anonymization

E) Vulnerability assessments and penetration testing

These techniques involve identifying and testing vulnerabilities in systems and networks to determine potential points of weakness that could be exploited by attackers.

E) Security information and event management (SIEM)

This involves collecting and analyzing security-related data from multiple sources to identify and respond to security threats in real-time [27].

VII. CHALLENGES OF DATA SECURITY IN IOT

The Internet of Things (IoT) is a rapidly growing field that involves the interconnection of various devices and systems, allowing them to exchange data and work together to perform complex tasks. With the increasing use of intelligent agents in IoT, there are several challenges related to data security. Some of these challenges are:

A) Authentication and Authorization

One of the major challenges in IoT security is ensuring that only authorized entities can access the data. Intelligent agents must be able to authenticate and authorize the devices and users accessing the data to prevent unauthorized access.

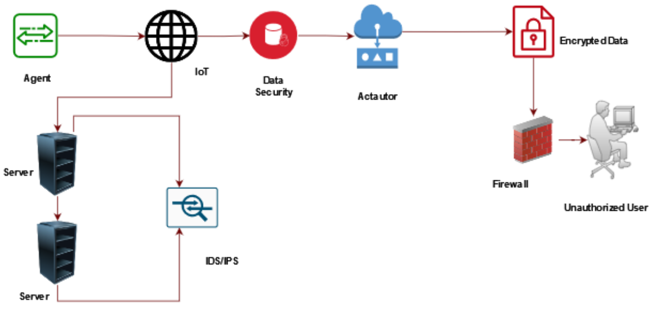

Fig. 4. Data Security Protection Architecture from Unauthorized User

A) Encryption

Encryption is essential to ensure that the data transmitted between devices and systems are secure. Intelligent agents must be able to encrypt the data to protect it from interception and ensure that it cannot be read by unauthorized parties.

B) Data Privacy

IoT devices often collect and transmit sensitive data such as personal and financial information. Intelligent agents must ensure that this data is protected from unauthorized access and is handled in compliance with data privacy regulations.

C) Device Security

IoT devices can be vulnerable to cyber-attacks, which can compromise the security of the entire network. Intelligent agents must be able to identify and respond to potential security threats in real time to ensure the security of the devices and the network as a whole.

D) Interoperability

IoT devices often come from different manufacturers and use different communication protocols, making it difficult for intelligent agents to communicate with them. Interoperability is essential for intelligent agents to effectively manage and secure the IoT network.

Overall, the challenges of data security in IoT with respect to intelligent agents are complex and constantly evolving. As the field continues to grow and new threats emerge, it is essential that intelligent agents remain up-to-date with the latest security protocols and technologies to ensure the security of the network and the data it transmits.

VIII. ISSUES OF DATA SECURITY IN IOT

Data security is a critical concern in the field of IoT, and the use of intelligent agents can present a range of issues related to security [28]. Some of the key issues of data security in IoT with respect to intelligent agents are:

A) Lack of Standardization

There is a lack of standardization in the field of IoT, and this can make it difficult for intelligent agents to ensure that data is transmitted and stored securely. Different devices and systems may use different communication protocols, making it challenging to establish secure connections and exchange data securely.

B) Vulnerabilities in Intelligent Agents

Intelligent agents can themselves be vulnerable to cyberattacks and data breaches, which can compromise the security of the entire IoT network. These vulnerabilities may arise from weaknesses in the code or in the way the agents are configured and managed.

C) Complexity

The complexity of the IoT network can also present challenges for data security. With numerous devices and systems connected to the network, there are multiple points of entry that attackers can exploit. The use of intelligent agents can further increase this complexity, as agents may interact with multiple devices and systems, making it difficult to track and manage data flows.

D) Lack of Awareness

There is often a lack of awareness among IoT users and stakeholders about the importance of data security. This can result in devices and systems being left vulnerable to cyberattacks or data breaches, potentially compromising the security and privacy of sensitive data.

E) Privacy Concerns

The use of intelligent agents can raise privacy concerns, as these agents may collect and process sensitive data about users and their behavior. This data must be handled carefully to ensure that privacy is protected, and users are not put at risk of identity theft or other forms of cybercrime.

Overall, the issues of data security in IoT with respect to intelligent agents are complex and multifaceted [29]. It is important that IoT stakeholders work together to establish clear security protocols and best practices, to ensure that intelligent agents can operate securely and protect the privacy and security of IoT data.

IX. SOLUTIONS TO DATA SECURITY ISSUES IN IOT

The issues and challenges of data security in IoT can be addressed through a combination of technological solutions and best practices [30]. The following are some solutions that can be implemented concerning intelligent agents:

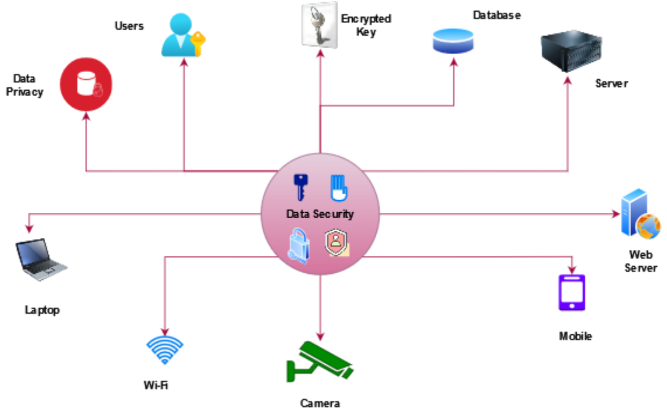

Fig. 5. Data Security with its Modules

A) Encryption

Data encryption is an essential security measure that can be implemented to protect data from unauthorized access. Intelligent agents can use encryption techniques to secure data as it is transmitted between devices and servers.

B) Authentication and Access Control

Implementing strong authentication mechanisms and access control policies can prevent unauthorized access to IoT devices and data. Intelligent agents can be designed to use secure authentication protocols such as OAuth or OpenID Connect to verify the identity of users and devices.

C) Intrusion Detection and Prevention

Intrusion detection and prevention systems (IDPS) can be used to identify and prevent malicious activity on IoT networks. Intelligent agents can be designed to monitor network traffic and identify anomalies that may indicate a security breach.

D) Standardization

Standards and protocols for IoT devices and communication can be developed and adopted, enabling intelligent agents to establish secure connections and exchange data securely. Efforts are already underway in various organizations and standards bodies to address this challenge, such as the Open Connectivity Foundation and the Industrial Internet Consortium.

E) Vulnerabilities in Intelligent Agents

Regular security assessments and testing can be conducted to identify and address potential vulnerabilities in intelligent agents. Regular updates and patches can also be provided to keep agents secure and up-to-date with the latest security protocols.

F) Complexity

Effective network segmentation, access control, and monitoring can be implemented to reduce the complexity of the IoT network and limit the potential attack surface for cyber-attacks. Intelligent agents can also be designed to use simpler and more secure communication protocols to reduce complexity.

G) Awareness

IoT stakeholders, including manufacturers, developers, and end-users, can be educated about the importance of data security and privacy in IoT. This education can include best practices for securing IoT devices and data, as well as awareness of the potential risks of cyber-attacks and data breaches.

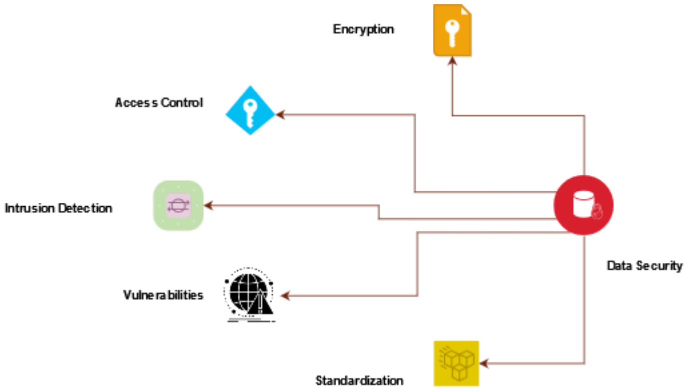

Fig. 6. Multiple Solutions used in IoT Data Security to Protect Data

TABLE II
COMPARATIVE SECURITY ANALYSIS OF ADVANCED TECHNOLOGIES USED FOR DATA SECURITY IN IOT

Network Models	Methodology	Percentage
Blockchain	Algorithms	93
Machine Learning	Security decentralization	89
Edge Computing	Networking	92
Zero-trust security	Networking	90
Machine Learning	Algorithm	94

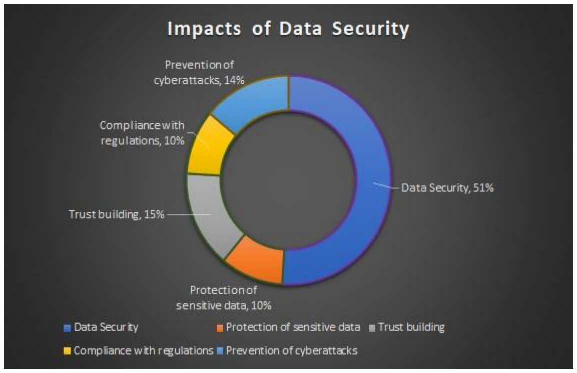

Fig. 7. Impact of Data Security in IoT

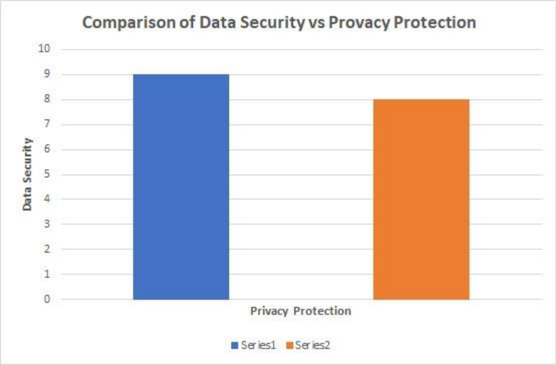

Fig. 8. Comparison between Data Security and Real-Time Threat Detection and Response

H) Privacy Concerns

Privacy-by-design principles can be applied to the development of intelligent agents, ensuring that user data is protected by default. This can include implementing strong encryption, access controls, and data minimization strategies to limit the collection and processing of sensitive data. Compliance with privacy regulations such as GDPR and CCPA can also be ensured.

Overall, a combination of technological solutions, best practices, and awareness-raising efforts can be employed to address the challenges and issues related to data security in IoT concerning intelligent agents [31]. These efforts can help ensure that IoT devices and networks are secure and that user data is protected.

X. ADVANCED TECHNOLOGIES USED FOR DATA SECURITY IN IOT CONCERNING INTELLIGENT AGENTS

There are several advanced solutions to data security issues in IoT concerning intelligent agents, including:

A) Blockchain technology

Blockchain is a decentralized, distributed ledger that can be used to securely store data and transactions [32]. By using blockchain technology, IoT devices, and intelligent agents can maintain a tamper-proof record of all data and transactions, ensuring the integrity and security of the data.

B) Machine learning-based anomaly detection

Machine learning algorithms can be used to identify and detect anomalous behavior in IoT devices and intelligent agents, helping to prevent cyber-attacks and data breaches.

C) Edge computing

Edge computing involves processing data closer to the source, rather than transmitting it to a central server for processing. By using edge computing, IoT devices, and intelligent agents can reduce the amount of data that needs to be transmitted, reducing the risk of data breaches and improving data security.
the privacy and security of the data. By using homomorphic encryption, IoT devices, and intelligent agents can perform complex data processing tasks without exposing the data to potential cyber-attacks.

Overall, the use of advanced technologies and approaches can help to address the complex data security issues in IoT concerning intelligent agents [33]. By adopting these solutions, IoT stakeholders can ensure the integrity and security of IoT data, protecting the privacy and security of sensitive information.

XI. POSITIVE IMPACTS OF DATA SECURITY AND PRIVACY IN IOT

There are several positive impacts of data security and privacy in IoT, including:

A) Protection of sensitive data

IoT devices are often used to collect and store sensitive data such as personal and financial information [34]. Ensuring data security and privacy helps protect this information from unauthorized access and use, preventing potential harm to individuals or organizations.

B) Trust building

Data security and privacy measures can help build trust between users and IoT devices and services. This can lead to increased adoption of IoT technologies, which can drive innovation and economic growth.

C) Compliance with regulations

Many industries are subject to regulations that require data security and privacy protections, such as HIPAA in healthcare and GDPR in the European Union. Ensuring compliance with these regulations can help organizations avoid legal and financial penalties and reputational damage.

D) Prevention of cyberattacks

IoT devices are often targeted by cybercriminals seeking to gain access to sensitive data or use the devices for malicious purposes. Implementing data security and privacy measures can help prevent these attacks and protect both users and organizations.

E) Improved operational efficiency

Data security and privacy measures can also improve operational efficiency by reducing the risk of downtime or data loss due to security breaches or data leaks. This can help organizations save time and resources that would otherwise be spent on recovery efforts.

Overall, ensuring data security and privacy in IoT has numerous positive impacts, including protecting sensitive data, building trust, complying with regulations, preventing cyberattacks, and improving operational efficiency.

XII. DATA SECURITY VS REAL-TIME THREAT DETECTION AND RESPONSE

While all of the impacts, including real-time threat detection and response, automated security protocols, personalized security settings, and privacy protection, are important in IoT, data security is perhaps the most critical.

The reason for this is that IoT devices often collect and transmit sensitive data, such as personal information, financial information, or even health data [35]. If this data is not properly secured, it can be vulnerable to cyberattacks or other security breaches. These breaches can lead to financial losses, legal liabilities, reputational damage, and harm to individuals or organizations.

Moreover, ensuring data security in IoT requires a comprehensive approach that includes all of the other impacts, Real-time threat detection and response, automated security protocols, personalized security settings, and privacy protection are all important components of a comprehensive data security strategy.

For example, real-time threat detection and response can help prevent data breaches by quickly identifying and responding to security threats. Automated security protocols can help ensure that all IoT devices are properly secured and that security measures are consistently applied. Personalized security settings can help protect individual users and devices based on their unique needs and usage patterns [36]. Privacy protection can help ensure that sensitive data is only accessible to authorized parties and cannot be used for malicious purposes.

Overall, data security is important in IoT because it is the foundation on which all other security and privacy measures are built. Without proper data security, all other efforts to protect IoT devices and data will be ineffective.

XIII. DATA SECURITY VS PRIVACY PROTECTION

Data security and privacy protection are both critically important impacts of IoT. However, data security is arguably more important than privacy protection because it lays the foundation for protecting all other aspects of IoT, including privacy.

Data security refers to the protection of IoT data from unauthorized access, use, disclosure, modification, or destruction. It is essential for ensuring that sensitive information, such as personal and financial data, is not compromised [37]. Data security is crucial in preventing cyberattacks and other security breaches that can result in significant financial and reputational damage.

On the other hand, privacy protection refers to the protection of individual privacy and personal data. It involves ensuring that sensitive information is not accessed or used by unauthorized parties and is only collected and processed following relevant privacy laws and regulations [38].

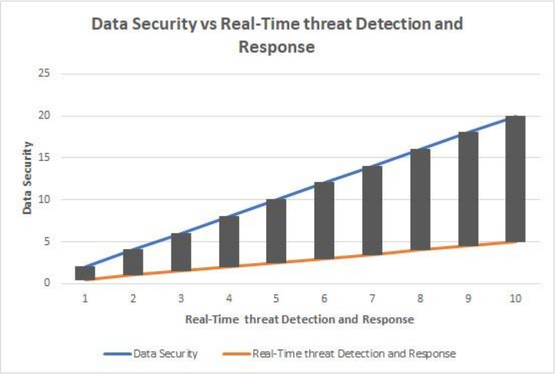

Fig. 9. Comparison between Data Security and Privacy Protection

While privacy protection is important, it depends on data security. If data security is compromised, then privacy protection measures become ineffective. For example, if a cybercriminal gains unauthorized access to sensitive data, they can use that data for nefarious purposes, regardless of whether privacy protection measures are in place.

In summary, while both data security and privacy protection are crucial for IoT, data security is more fundamental as it is the foundation on which privacy protection measures are built [39]. Therefore, ensuring robust data security is the first step towards protecting privacy in IoT.

XIV. FUTURE DIRECTION

The future direction of this field is to establish clear security protocols and best practices to ensure the security and privacy of IoT data. A collaborative effort is required to ensure that stakeholders are aware of the latest security protocols and technologies, and regular security assessments are conducted.

Additionally, compliance with privacy regulations and the use of privacy-by-design principles can be employed to protect user data. The paper suggests that a comprehensive data security strategy involving real-time threat detection and response, automated security protocols, personalized security settings, and privacy protection is needed to address the challenges of data security in IoT concerning intelligent agents. Overall, the future direction is to continue exploring new and innovative technologies and approaches to ensure the integrity and security of IoT data and protect the privacy and security of sensitive information.

XV. CONCLUSION

The paper concludes that data security is crucial in IoT, especially in the context of intelligent agents, due to the increasing number of devices and potential cyber threats. Various techniques and approaches, such as encryption, blockchain, machine learning, and zero-trust security, can be used to address data security issues in IoT. The paper also highlights the importance of collaborative efforts, compliance with regulations, and best practices to establish clear security protocols and protect user data. Additionally, the paper emphasizes that data security is more critical than privacy protection in IoT as it forms the foundation for protecting all other aspects of IoT, including privacy. Therefore, ensuring robust data security is the first step towards protecting privacy in IoT.

REFERENCES

[1] Coulter, Rory, and Lei Pan. ”Intelligent agents defending for an IoT world: A review.” Computers Security 73 (2018): 439-458.

[2] Abomhara, Mohamed, and Geir M. Køien. ”Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks.” Journal of Cyber Security and Mobility (2020): 65-88.

[3] Jing, Qi, et al. ”Security of the Internet of Things: perspectives and challenges.” Wireless Networks 20 (2019): 2481-2501.

[4] Tawalbeh, Lo'ai, et al. ”IoT Privacy and security: Challenges and solutions.” Applied Sciences 10.12 (2020): 4102.

[5] Musonda, Chalwe, et al. ”Security, Privacy and Integrity in Internet of Things–A Review.” Proceedings of the ICTSZ International Conference in ICTs. 2019.

[6] Nadikattu, Ashok Kumar Reddy. ”Iot and the Issue of Data Privacy.” International Journal of Innovations in Engineering Research and Technology 5.10 (2020): 23-26.

[7] Ogonji, Mark Mbock, George Okeyo, and Joseph Muliaro Wafula. ”A survey on privacy and security of Internet of Things.” Computer Science Review 38 (2020): 100312.

[8] Alhayani, Bilal, et al. ”Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry.” Materials Today: Proceedings 531 (2021).

[9] Inderwildi, Oliver, et al. ”The impact of intelligent cyber-physical systems on the decarbonization of energy.” Energy Environmental Science 13.3 (2020): 744-771.

[10] Naik, Binny, et al. ”The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review.” Complex Intelligent Systems 8.2 (2022): 1763-1780.

[11] Kuzlu, Murat, Corinne Fair, and Ozgur Guler. ”Role of artificial intelligence in the Internet of Things (IoT) cybersecurity.” Discover Internet of things 1 (2021): 1-14.

[12] Li, Jingfu. ”IOT security analysis of BDT-SVM multi-classification algorithm.” International Journal of Computers and Applications 45.2 (2023): 170-179.

[13] Chandol, Mohan Kumar, and M. Kameswara Rao. ”Blockchain-based cryptographic approach for privacy enabled data integrity model for IoT healthcare.” Journal of Experimental Theoretical Artificial Intelligence (2023): 1-22

[14] Zhang, Xiaohong, and Xiaofeng Chen. ”Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network.” Ieee Access 7 (2019): 58241-58254

[15] Mai, Xiaoqing, et al. ”Security protection method of power system database based on cloud platform.” International Conference on Statistics, Data Science, and Computational Intelligence (CSDSCI 2022). Vol. 12510. SPIE, 2023.

[16] Han, Pengchong, et al. ”Access control mechanism for the Internet of Things based on blockchain and inner product encryption.” Journal of Information Security and Applications 74 (2023): 103446.

[17] Huang, Teng, et al. ”Smart contract watermarking based on code obfuscation.” Information Sciences 628 (2023): 439-448.

[18] Wu, Nannan, Lei Xu, and Liehuang Zhu. ”A blockchain based access control scheme with hidden policy and attribute.” Future Generation Computer Systems 141 (2023): 186-196.

[19] Nadikattu, Ashok Kumar Reddy. ”Iot and the Issue of Data Privacy.” International Journal of Innovations in Engineering Research and Technology 5.10 (2020): 23-26.

[20] Ogonji, Mark Mbock, George Okeyo, and Joseph Muliaro Wafula. ”A survey on privacy and security of Internet of Things.” Computer Science Review 38 (2020): 100312.

[21] Kuzlu, Murat, Corinne Fair, and Ozgur Guler. ”Role of artificial intelligence in the Internet of Things (IoT) cybersecurity.” Discover Internet of things 1 (2021): 1-14.

[22] Musonda, Chalwe, et al. ”Security, Privacy and Integrity in Internet of Things–A Review.” Proceedings of the ICTSZ International Conference in ICTs. 2019.

[23] Kyle Johnson.” top 7 types of data security technology.” Proceedings of the ICTSZ International Conference in ICTs. 2022

[24] Alasmari, Sultan, and Mohd Anwar. ”Security privacy challenges in IoTbased health cloud.” 2016 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2021.

[25] Coulter, Rory, and Lei Pan. ”Intelligent agents defending for an IoT world: A review.” Computers Security 73 (2018): 439-458.

[26] Abomhara, Mohamed, and Geir M. Køien. ”Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks.” Journal of Cyber Security and Mobility (2019): 65-88.

[27] 27. Tawalbeh, Lo'ai, et al. ”IoT Privacy and security: Challenges and solutions.” Applied Sciences 10.12 (2020): 4102.

[28] 28. Azrour, Mourade, et al. ”Internet of things security: challenges and key issues.” Security and Communication Networks 2021 (2021): 1-11.

[29] 29. Jing, Qi, et al. ”Security of the Internet of Things: perspectives and challenges.” Wireless Networks 20 (2019): 2481-2501.

[30] 30. Tawalbeh, Lo'ai, et al. ”IoT Privacy and security: Challenges and solutions.” Applied Sciences 10.12 (2020): 4102.

[31] 31. Medaglia, Carlo Maria, and Alexandru Serbanati. ”An overview of privacy and security issues in the internet of things.” The Internet of Things: 20 th Tyrrhenian Workshop on Digital Communications. Springer New York, 2020.

[32] 32. Naik, Binny, et al. ”The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review.” Complex Intelligent Systems 8.2 (2022): 1763-1780.

[33] 33. Alasmari, Sultan, and Mohd Anwar. ”Security privacy challenges in IoT-based health cloud.” 2016 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2016.

[34] 34. Coulter, Rory, and Lei Pan. ”Intelligent agents defending for an IoT world: A review.” Computers Security 73 (2018): 439-458.

[35] 35. Abomhara, Mohamed, and Geir M. Køien. ”Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks.” Journal of Cyber Security and Mobility (2015): 65-88.

[36] 36. Siegel, Joshua E., Sumeet Kumar, and Sanjay E. Sarma. ”The future internet of things: secure, efficient, and model-based.” IEEE Internet of Things Journal 5.4 (2017): 2386-2398.

[37] 37. Siegel, Joshua E., Sumeet Kumar, and Sanjay E. Sarma. ”The future internet of things: secure, efficient, and model-based.” IEEE Internet of Things Journal 5.4 (2017): 2386-2398.

[38] 38. Alhayani, Bilal, et al. ”Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry.” Materials Today: Proceedings 531 (2021).

[39] 39. Inderwildi, Oliver, et al. ”The impact of intelligent cyber-physical systems on the decarbonization of energy.” Energy Environmental Science 13.3 (2020): 744-771.