Block Chain Based Secure Routing and Trust Management in Wireless Sensor Networks

Gowri ShankarC[1]Kumar S[2]Kavinesh K[3]Lokendran S[4]SukumarV[5]
Prof& Head in DepartmentofECE, KSRCE TIRUNCHENGODE, TamilNadu, India
[2,3,4,5]StudentinDept.ofECE,KSRCETIRUCHENGODE,TamilNadu,India

***Abstract* -On the basis of a blockchain that stores the identities of the Aggregator Nodes (ANs) and Sensor Nodes (SNs), an encryption and trust evaluation model is proposed. ANs and SNs are authenticated on private and public blockchains, respectively. However, hostile actions are carried out by untrusted nodes who use network resources. The SNs are also vulnerable to attacks from malicious nodes and have low energy, transmission range, and computing capabilities. The malicious nodes then communicate inaccurate route information and increase the amount of retransmissions, which causes the SNs' energy to be quickly used up. The quick energy dissipation of the SNs shortens the lifespan of the wireless sensor network. Additionally, the throughput and packet loss both rise in response to thea network's harmful nodes. To remove malicious nodes from the network, the trust values of SNs are computed. In order to accomplish secure routing, the network takes into account the SNs' trust values and remaining energy. Additionally, asymmetric key cryptosystem Rivest-Shamir-Adleman (RSA) is employed to secure data transfer. The simulation results demonstrate the suggested model's usefulness in terms of a high packet delivery ratio.**

As seen by a recent wave of widely reported events where users unintentionally exposed personal information, ensuring privacy has become a significant challenge as a result of the growing volume of photos users upload on social media. These occurrences make it clear that technologies are needed to enable people manage access to their shared content. To help users create privacy settings for their photographs, users offer the Adaptive Privacy Policy Prediction (A3P) system. Users suggest a two-level framework that decides the optimum privacy policy for the user's photographs based on the user's history on the site uploaded. In order to automatically develop a policy for each freshly uploaded image, also in accordance with users' social attributes, our approach relies on a policy prediction algorithm and an image classification framework for image categories that may be related with similar policies. The produced policies will adjust as users' attitudes towards privacy change over time. Users submit the findings from our thorough analysis of more than 5,000 policies, which show the efficiency of our system with prediction accuracies over 90%.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is crucial to the development of many applications, including those in the military, the healthcare industry, industrial monitoring, etc. Randomly dispersed Sensor Nodes (SNs) with limited energy, storage, and computing capabilities make up this self-organized network. The SNs track a variety of variables, including wind, humidity, temperature, etc., and then transmit the information to the Base Stations. (BSs). Security concerns are one of the main issues with WSNs. The cause is that SNs have limited resources and are vulnerable to attack. There are typically two sorts of assaults carried out in WSNs. Internal attacks occur when SNs act selfishly to protect their energy and storage, as opposed to external attacks, in which the attackers seize control of the SNs to carry out nefarious operations.Therefore, it is essential to locate and eliminate the malicious nodes from the network.

II. LITERATURESURVEY

a) Tag, you can see it! using tags for access control in photo sharing

Users frequently have sophisticated and intricate photo-sharing preferences, but setting up access control correctly can be challenging and time-consuming. In a laboratory study involving 18 participants, we investigate the possibility of using the tags users give their images to make it easier for users to maintain and implement access-control policies. We find that (a) tags made for organisational purposes can be used to make effective and reasonably accurate access-control rules; (b) users who tag with access control in mind develop coherent strategies that result in rules that are significantly more accurate than those associated with organisational tags alone; and (c) tags made for organisational purposes can be used to make rules for other purposes.

b) Understanding privacy settings in face book with an audience view

Users of online social networking communities are disclosing large amounts of personal information, putting themselves at a variety of risks. Our ongoing research investigates mechanisms for socially appropriate privacy management in online social networking communities. As a first step, we are examining the role of interface usability in current privacy settings. In this paper we report on our first iterative prototype, where presenting an audience-oriented view of profile information significantly improved the understanding of privacy settings.

c) The PViz comprehension tool for social network privacy settings

Subgroups inside users' personal networks of friends frequently figure into their conceptions of privacy and visibility on social networks. Many social networking services, like Facebook's lists and "Smart Lists" and Google+'s "Circles," have started developing user interfaces to facilitate grouping. However, current tools for understanding policy, like Facebook's Audience View, are not compatible with this mental paradigm. In this research, we introduce PViz, an interface and technology that more closely matches users' modelling of network groups and privacy regulations. With the help of multiple levels of granularity and automatically created, natural friend subgroupings, PViz enables the user to comprehend the visibility of her profile. We also tackle the crucial sub-problem of creating accurate group labels because the user must be able to recognise and distinguish automatically-constructed groupings. We ran a thorough user study contrasting PViz with the most popular tools for understanding policy at the moment (Facebook's Audience View and Custom Settings page). Our research showed that, although requiring users to become used to a new tool, PViz was similar to Audience View for simple activities and offered a significant improvement for complicated, group-based tasks.

III PROPOSEDSYSTEM

WSNs have made significant contributions to the growth of numerous fields, including industrial surveillance, the military, and healthcare. However, the networks face a variety of difficult problems. In order to identify malicious nodes, the authors in used a block chain based methodology. Due to the usage of the PoW consensus process, the model has a significant computational cost. Additionally, nodes' authentication is skipped, allowing unauthorised nodes to use and access network resources. On the basis of data and behaviour-based trust, a blockchain-based trust paradigm is suggested. However, in data-based trust, recommender nodes are used to evaluate indirect trust. When the recommender nodes are malicious, inaccurate information about the network's trustworthy nodes is sent. The secure route is found by the WSN using a suggested routing technique. The authors, however, do not take into account the detection and authentication of the rogue nodes. The malicious nodes delete the packets that lead to a poor Packet Delivery Ratio (PDR) by faking the real identities of the benign nodes. The increased energy usage when forwarding data packets to neighbours also has a negative impact on the network's lifespan. Additionally, both packet encryption and decryption employ a symmetric key. However, a third party can readily obtain the encryption key using the symmetric key and use it to decrypt the packets in order to recover the original data. To authenticate the nodes in the IoT network, an authentication protocol is proposed.. When it gets message acknowledgment, the BS gives each SN a sequence number. However, while assigning Sensors 2022, 22, 411 7 of 24 sequence numbers, the BS does not check the credentials of the SNs. This consequently enhances the likelihood that the malicious nodes will join the network.

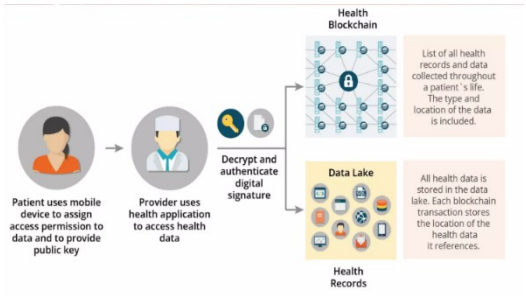

Fig 3.1 diagram for proposed system

1.Advantages

It might not be enough to analyse the visual content to determine consumers' privacy preferences. In addition to providing a synthetic description of photos and completing the knowledge gained via visual content analysis, tags and other metadata are suggestive of the social context of the image, including where it was taken and why.

• The user-friendly privacy policy settings for uploaded photographs are effectively automated by our suggested work.

2. Feasibility study:
The project's viability and the possibility that the system will be helpful to the organisation are both examined in the preliminary investigation. The major goal of the feasibility study is to determine whether it is technically, operationally, and economically feasible to add new modules and fix existing systems. If there have infinite resources and time, every system is viable. There are elements in the preliminary investigation's feasibility assessment.

- Economical Feasibility
- Operation Feasibility
- Technical Feasibility.

2.1 Economical Feasibility:
Although a system can be created technically, the organisation must still consider it a good investment if it is to be employed. The development cost of developing the system is weighed against the final benefit received from the new systems in the economic feasibility analysis. Benefits must match or surpass expenditures in terms of money.
2.2 Operation Feasibility:

Only projects that can be converted into information systems are worthwhile. This will satisfy the organisation's operational needs. Project execution must consider the operational feasibility considerations as a key component. To test a project's operational viability, some crucial problems are raised, such as the following:
• Do the users provide the management with enough support?
• If the system is being created and put into use, will it be used and function properly?
• Will the user's resistance thwart the potential advantages of the application?

2.3 *technical feasibility:*
The following are some of the technical issues that are typically brought up during the feasibility stage of the investigation:
• Is the technology required to carry out the suggestion already available?
• Can the suggested equipment technically store the data needed to operate the new system?
• Regardless of the quantity or location of users, will the proposed system be able to adequately respond to queries?
• If developed, can the system be upgraded?
Are there technical assurances of correctness, dependability, accessibility, and data security?

Flow Chart

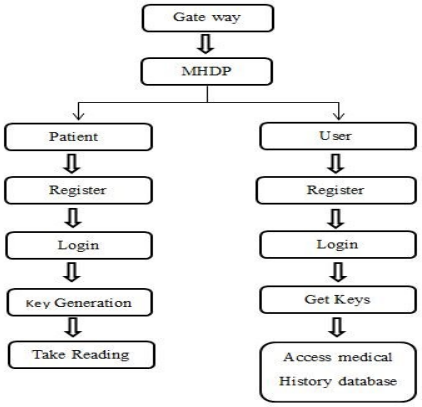

Fig3.2 .Flowchartforouroveralloperation

SOFTWARE DESCRIPTION

1. FRONTEND

JAVA DESCRIPTION

Java is a straightforward but effective object-oriented programming language that has many characteristics with C++. In 1991, Sun Microsystems, Inc. was where Java first appeared. James Gosling, Patrick Naughton, Chris Warth, Ed Frank, and Mike Sheridan from Sun Microsystems, Inc. came up with the idea. It was created to offer a programming language that is independent of operating systems.

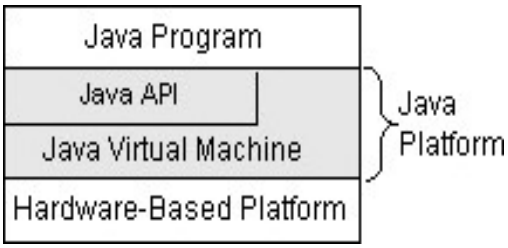

Fig 3.2 javaprogramand hardware

Platform independent

When Java is compiled, unlike many other programming languages, such as C and C++, it is not compiled into platform-specific machine code but rather into platform-independent byte code. On whatever platform that is being used, virtual Machine (JVM) on the web distributes this byte code and interprets it.

A. Java Virtual Machine

Java was created with the idea of "write once, run anywhere." The Java Virtual Machine is essential to this idea. The setting in which Java programmes run is called the JVM. On top of actual hardware and an operating system, it is software. After being converted into byte codes during compilation, the source code (.java files) is stored into (.class) files. These bytecodes are executed by the JVM. Therefore, Java byte codes can be viewed as the JVM's machine language. A just-in-time compiler is used to further compile the bytecode for the actual CPU, or a JVM can parse the bytecode one instruction at a time.

1. Abstraction

According to the viewpoint of the spectator, abstraction refers to an object's fundamental qualities that set it apart from all other kinds of things and, as a result, establish clearly defined conceptual limits.Abstraction is the process of separating abstract concepts from concrete applications of those concepts. While obscuring the specifics of how they operate, computational structures are defined by the meanings (semantics) they convey. Abstraction attempts to factor out specifics from a common pattern to bring programming closer to the level of human intellect by omitting specifics that are important in practice but irrelevant to the problem at hand.When a system has many abstraction layers, for instance, the programmer is exposed to different meanings and levels of detail; for instance, low-level layers provide information about the computer hardware on which the program runs, whilst high-level layers deal with the program's business logic.

2. Encapsulation

Encapsulation is the process of compartmentalising an abstraction's constituent structural and behavioural pieces; it serves to distinguish an abstraction's contractual interface from its implementation. Data and functions are combined into a single component through encapsulation. Although there are other options, most object-oriented programming languages use classes to support the characteristics of encapsulation. By creating an impermeable wall to shield the code from unintentional corruption, it enables for the selective hiding of attributes and methods in an object. The three cornerstones of object-oriented programming are encapsulation, inheritance, and polymorphism.

3. Inheritance

The process through which one item gets the properties of another object is known as inheritance. When an object or class is based on another object or class, inheritance occurs. This might happen when an interface is realised or when an implementation is specified to preserve the same functionality. It serves as a method for code reuse and for permitting independent software extensions through public classes and interfaces. A hierarchy results from the connections between objects or classes through inheritance. For Simula, inheritance was created in 1967. Subtyping and inheritance should not be confused.In general, subtyping establishes an ins-a relationship while inheritance only reuses implementation and establishes a syntactic relationship, not necessarily a semantic

relationship (inheritance does not ensure behavioural subtyping). In some languages inheritance and subtyping are compatible, while they are not in others.

SOCKET OVERVIEW:
A network socket is a lot like an electrical socket. Various plugs around the network have a standard way of delivering their payload. Anything that understands the standard protocol can “plug in” to the socket and communicate.
Internet protocol (IP) is a low-level routing protocol that breaks data into small packets and sends them to an address across a network, which does not guarantee to deliver said packets to the destination.
Transmission Control Protocol (TCP) is a higher-level protocol that manages to reliably transmit data. A third protocol, User DatagramProtocol (UDP), sits next to TCP and can be used directly to support fast, connectionless, unreliable transport of packets.

CLIENT/SERVER:
A server is anything that has some resource that can be shared. There are compute servers, which provide computing power; print servers, which manage a collection of printers; disk servers, which provide networked disk space; and web servers, which store web pages. A clientis simply any other entity that wants to gain access to a particular server. A server process is said to “listen” to a port until a client connects to it. A server is allowed to accept multiple clients connected to the same port number, although each session is unique. To mange multiple client connections, a server process must be multithreaded or have some other means of multiplexing the simultaneous I/O.

PROJECT DESCRIPTION

A. PROBLEM DEFINITION

When attempting to use data that contains sensitive information about specific individuals, privacy is a major issue. Many academic disciplines, including computer science, statistics, economics, and social science, have contributed to the research on protecting individual privacy and the confidentiality of information. In this essay, we review studies on releasing facts while protecting privacy. A solution to the problem of how a company, such as a hospital, government agency, or coverage company, can disseminate information to the public without infringing the confidentiality of private information is attempted in this field.We discuss techniques to read the sanitised statistics, describe algorithms that sanitise the data to make it safe for dissemination while maintaining important information, and recognise privacy criteria that offer formal safety guarantees. There are still many challenging scenarios. This survey provides a summary of the state-of-the-art as of right now, which serves as the foundation for anticipating future advancements.

OVERVIEW OF THE PROJECT
Social media has reportedly had an impact on communication within society and public discourse in recent years. Particularly, social media is being used more and more in political context. More recently, social networking sites like Facebook and microblogging services like twitter are thought to have the potential to increase political participation. While political institutions (such as politicians, political parties, political foundations, etc.) have started to use Facebook pages or agencies in order to engage in direct dialogue with citizens and promote more political discussions, Twitter is still a great platform for users to disseminate news in general as well as political evaluations publicly through their networks. Previous research has demonstrated that there may be an increasing need to continuously gather, monitor, evaluate, synthesize, and visualise politically relevant facts from social media based on the attitude of political institutions. These duties, which fall under the category of "social media analytics," are seen as difficult due to the wide variety of social media platforms as well as the vast amount and complexity of statistics and data. There is still a lack of systematic tracking and analytic methods together with appropriate scientific methods and strategies in the field of politics. We provide a methodological framework for social media analytics in a political setting in this study. More specifically, our framework summarises the most important issues that are politically significant based on political establishment attitudes and corresponding approaches from unique medical specialties.

SYSTEM TESTING

1) UNIT TESTING

Unit testing concentrates verification efforts on the module, which is the smallest unit of software design. "Module testing" is another name for this.Each module is tested independently. This testing is done right together with the

code. Each module is found to be functioning satisfactorily in this testing phase with reference to the module's anticipated output.

2) TESTING

Integration testing is a methodical testing for building the programme structure. Data can be lost over an interface, one module can negatively impact others, sub-functions when integrated may not generate the required principal functions, and integration testing can cause data to be lost across an interface. In addition, are you also looking for interface-related errors? The goal is to combine unit-tested modules and test the system as a whole. The enormous costs of the entire programme make it difficult to isolate the causes in this situation, making repair challenging. All faults found during this integration testing stage are fixed in preparation for the following testing stage.

3) SYSTEM TESTING

Before the system goes into live operation, accuracy and efficiency are checked by system testing, which is a stage of implementation. The system's success depends on testing. System testing makes the logical premise that the objective will be effectively attained if every component of the system is correct. A number of tests are run on the candidate system. Before the proposed system is ready for user acceptability testing, a number of tests are run on it..

The testing steps are:

- Validation testing
- Output testing
- User acceptance testing

4) VALIDATION TESTING

Verification testing operates the system with simulated data in a simulated environment. Many times, alpha testing is used to describe this simulated test. The main goal of this simulated test is to find mistakes and conclusions about end-user behaviour and design requirements that were specified in the preliminary stages but were not met throughout development.

Validation is the process of utilising software in a real setting to detect faults. The programme is typically changed in response to feedback from the validation phase to address problems and failures that are discovered. The system is then put to use on a live basis by a selection of user sites. They're known as beta tests.

The beta test participants use the system in regular use. They carry out real-time transactions and generate standard system output. The users are aware they are using a system that may malfunction, therefore the system is live in every sense of the word. However, the transactions entered and the users of the system are actual people. Validation might go on for a while. Failure may occur when the system is being validated, in which case the programme will be modified. The need for more adjustments and new failures could result from continued use.

5) OUTPUT TESTING

The suggested system's output testing comes after doing the validation because no system can be useful if it cannot deliver the necessary output in the needed format. The output produced or displayed by the system under consideration is tested by asking the users about the format they desire. As a result, there are two ways to think about the output format: one is on a screen, and the other is in printed form.

III. CONCLUSION

An integrated development environment (ide) for Java is called Netbeans. Applications can be created with Netbeans using a collection of modular software components known as modules. Windows, Mac OS X, Linux, and Solaris all support Netbeans.An integrated development environment (ide) for Java is called Netbeans. Applications can be created with Netbeans using a collection of modular software components known as modules. Windows, Mac OS X, Linux, and Solaris all support Netbeans. It contains extensions for languages like php, c, c++, html5, and javac script in addition to java development. The Netbeans IDE and any applications built on it can be expanded by other developers. Under the direction of the faculty of mathematics and physics at Charles university in Prague, Netbeans was first developed in 1996 as xelfi (a play on the word Delphi), a Java IDE student project. Roman Stank established a business around the project in 1997, producing commercial iterations of the NetBeans IDE until Sun Microsystems acquired it in 1999. In June of the following year, Sun made the Netbeans ide open-source. The netbeans community has expanded ever since. Oracle Corporation purchased Sun in 2010 (and subsequently Netbeans). Developer, a freeware ide that was formerly a corporate product, competed with Netbeans under Oracle. Oracle proposed giving the Netbeans project to the Apache Software Foundation in September 2016. According to Oracle,through the upcoming release of Java 9 and Netbeans 9 and beyond, opening up the Netbeans governance

model to allow Netbeans stakeholders a greater role in the project's direction and future success. James Gosling, the man who invented Java, supported the action. In October 2016, the project was accepted into the Apache incubator. With the release of Netbeans ide 6.9 in June 2010, additional features like as faster code navigation (such as "is overridden/implemented" annotations), formatting, suggestions, and refactoring across many languages were made available.

REFERENCES

[1] P. Klemperer, Y. Liang and M. Mazurek et al., (2022) “Tag, you can see it!: Using tags for access control in photo sharing,” in Proc. ACM Annu Conf. Human Factors Comput. Syst., pp. 377–386.

[2] H. Lipford, A. Besmer, and J. Watson (2021) “Understanding privacy settings in facebook with an audience view,” in Proc. Conf. Usability, Psychol., Security.

[3] A. Mazzia, K. LeFevreand A. E., (2020) “The PViz comprehension tool for social network privacy settings,” in Proc. Symp. Usable Privacy Security.

[4] J. Bonneau, J. Anderson, and G. Danezis (2021) “Prying data out of a social network,” in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining., pp.249–254.

[5] A. Vailaya, A. Jain, and H. J. Zhang (2021) “Image classification: City images vs. Landscapes” Pattern Recog. [Online]. 31(12), pp. 1921–1935.Available: http://www.sciencedirect.com/science/article/pii/S003132039800079X.

[6] J. Zhuang and S. C. H. Hoi (2021) “Non-parametric kernel ranking approach for social image retrieval,” in Proc. ACM Int. Conf. Image Video Retrieval, pp. 26–33. [Online]. Available: http://doi.acm.org/10.1145/1816041.1816047

[7] M. D. Choudhury, H. Sundaramand D. D. Seligmann (2021) “Connecting content to community in social media via image content, user tags and user communication,” in Proc. IEEE Int. Conf. Multimedia Expo, pp.1238–1241.

[8] Analysing Facebook features to support event detection for photo-based Facebook applications (Mohammad Rabbath, Philipp Sandhaus, Susanne Boll), In International Conference on Multimedia Retrieval, ICMR ’12, Hong Kong, China, June 5-8, 2012, 2022.

[9] H. Sundaram, L. Xie and M. De Choudhury (2021) “Multimedia semantics: Interactions between content and community” Proc. IEEE, vol. 100, no. 9, pp. 2737–2758, Sep.

[10] R. da Silva Torres and A. Falco (2021) “Content-based image retrieval: Theory and applications,” Revista de InformaticaTeorica e Aplicada, vol. 2, no. 13, pp. 161–185.