Personal and Ubiquitous Computing (2023) 27:119–137
https://doi.org/10.1007/s00779-022-01665-1

ORIGINAL ARTICLE

Artificial general intelligence-based rational behavior detection using cognitive correlates for tracking online harms

Shahid Naseem[1] · Adi Alhudhaif[2] · Muhammad Anwar[3] · Kashif Naseer Qureshi[4] · Gwanggil Jeon[5]

Received: 1 February 2021 / Accepted: 10 January 2022 / Published online: 21 January 2022

Abstract

Expert systems possess human-like expertise for data analyzing as well as for decision-making. These systems are suitable in a situation, where a high level of uncertainty exists. In expert systems, for protecting sensitive information, various encryption techniques such as classical encryption and quantum encryption are used. In these systems, Artificial Intelligence (AI) is used to analyze the data at runtime and to detect unauthorized users in the early stage especially for tracking online harms. These systems are not completely secured, because the encryption techniques have some loopholes such as the algorithm's short life expectancy and less computation power. An unauthorized user destroys the precious data, as well as the system, might access these loopholes. As the confidentiality and integrity of expert systems are threatened by intrusions and real-time attacks related to privacy and cyber-security, there is a need for proposing novel methodologies to predict future attacks and identify new threat patterns. To analyze the behavior of the intruder and overcome the encryption weaknesses, this paper presents an Artificial General Intelligence-based Rational Behavior Detection Agent (AGI-RBDA). The proposed system possesses human-like rationality for protecting the information like a human mind. It is exposed that the human mind does not apply any kind of encryption technique; instead, it used various cognitive correlates such as intention, perception, motivation, emotions, and implicit and explicit knowledge for the secrecy of sensitive information. In the end, the behavior of different cognitive correlates is exposed and stimulated.

Keywords Cognitive agent · Behavior analysis · Artificial intelligence · Artificial general intelligence

1 Introduction

With the expanding growth of the Internet and social media, security challenges to different applications and services are increasing day-by-day [1, 2]. In networks and information security systems, vulnerability and threats are not only big security issues but also can restrict further progress in the world's network economy. Network security not only secures the end user's data but also secures the entire network. In digital systems, for protecting the user's as well as the organization's sensitive data, several security measures such as firewalls, passwords, intrusion detection policies, and data recovery plans are introduced in the digital systems. The expert systems are used for decision-making by using artificial intelligence to solve the complex problems for rational behavior detection and are also capable of analyzing the unknown attacks at runtime and taking actions against these attacks to find an optimal solution [3, 4]. These systems rely on training data; as such, their performance deteriorates in the absence of a labeled training set, rendering single classifiers inadequate to cope

✉ Gwanggil Jeon
gjeon@inu.ac.kr

Shahid Naseem
shahid.naseem@ue.edu.pk

Adi Alhudhaif
a.alhudhaif@psau.edu.sa

Muhammad Anwar
anwar.muhammad@ue.edu.pk

Kashif Naseer Qureshi
kashifnq@gmail.com

[1] Department of Information Science, University of Education, Lahore, Pakistan

[2] Department of Computer Science, College of Computer Engineering and Sciences in Al-kharj, Prince Sattam bin Abdulaziz University, P.O. Box 151, Al-kharj 11942, Saudi Arabia

[3] Department of Information Science, University of Education, Faisalabad, Pakistan

[4] Department of Computer Science, Bahria University, Islamabad, Pakistan

[5] Department of Embedded Systems Engineering, Incheon National University, Incheon, South Korea

with zero-day and other unknown attacks. These systems can also assist humans in controlling the security issues in the network that may cause or damage sensitive data. These systems ensure the authenticity, confidentiality, integrity, and availability of information continuously. These systems require a security management approach for real-time data analysis, capability, adoption, and generalization of possible attacks [5, 6]. In expert systems, artificial intelligence (AI) supports the exploration of malicious data at runtime. AI also supports reducing the damages caused by intruders and minimizing the data losses. AI also provides suggestions of what necessary measures are required to mitigate the risk factors [7, 8]. A real-time exploration allows the security system to prevent intruders at the initial state. The expert systems contain significant knowledge of human experts in a specific domain and rival their decision-making abilities in that area.

Artificial intelligence–based expert systems designed for security provision are using two cryptographic techniques including classical and quantum techniques that are used for protecting sensitive information. In classical cryptography, a secret key is used for protecting information transmitted from source to destination node [9, 10]. In this technique, data is converted into ciphertext using a public key at the source node before sending it to the destination node over the Internet, so that an unauthorized user cannot access the original data during transmission. At the destination node, the ciphertext data is converted into original data using a private key [11]. Quantum cryptography is more secure than classical cryptography. In quantum cryptography, data is transmitted from the source node to the destination node in the form of photons. In a source node, a public key is used to convert the photonic data into ciphertext using a public key, so that an eavesdropper cannot access the ciphertext during transmission over the Internet [12–14]. These systems are not completely secured, because the encryption techniques or algorithms have some limitations including short life expectancy and less computation power. An unauthorized user takes benefit from these limitations and destroys the precious data. To analyze the behavior of the intruder and overcome the encryption weaknesses, this paper presents an approach for protecting sensitive information before sharing it with the other agents using cognitive correlates like a human mind. An objective of this paper is to propose an Artificial General Intelligence-based Rational Behavior Detection Agent (AGI-RBDA). The proposed agent possesses human-like rationality for protecting sensitive information before sharing it with the other agents using cognitive correlates like a human mind. In this agent, the adopted cognitive factors such as intention, perception, motivation, emotions, and implicit and explicit knowledge for the secrecy of sensitive information play an important role in sharing sensitive information between agents. AGI-RBDA is proposed to develop the capabilities of thinking, learning, and decision-making in the system. It can infer the people's mental state pre-dispositions to a particular behavior. It can also provide human-like cognition such as the ability to think, learn, and speak to the machine in a cognitive agent.

The rest of the paper is organized as follows: Section 2 presents the related work and discussed the expert systems. Section 3 presents the design and development phases of the proposed system. Section 4 presents the results and discussion. The Paper concludes in the last section with future directions.

2 Related work

In expert systems, cryptography is one of the methods for data protection and data transmission in the network. Cryptography is working on layers especially in wireless communication where it protects the data with multiple components including network monitoring, networking, and software security and hardware devices [15]. The AI methods are used to train the detector and secure the data by considering security issues such as detecting malicious activities on the web. The AI methods are also used for predicting the user's vulnerabilities and protecting them from social security attacks [16]. The AI-based expert systems are working and thinking like humans. As discussed in [17], cognitive science in an expert system is used in the human mind especially for complex tasks. NeuroNet is one of the methods for data collection and processing the distributed data for further coordination. This method also analyzes the irregularities or networks and intimates the systems for further countermeasures. This method is working well against the Denial of Service (DoS) attacks [18]. Security systems are based on AI for detection and analyzing unknown attacks in the network. These security systems collect the information and then analyze and suggest the actions more effectively.

AGI is helpful to achieve rationality especially like a human mind's behavior to solve the problems for further decision-making and information sharing. The cognitive agent rationality is used for cognitive processes. It is important to make agents cognitive; the users must understand human intelligence and all the difficulties to incorporate to achieve cognition in agency [1]. Esser and Haider in [19], discussed the explicit knowledge acquired from learning without explicit knowledge. In another study [20], the authors discuss two types of knowledge that are interlinked with each other. The theory of conscious mind is used for the self-identity and unconscious mind. Authors in [17], discussed the idea of Cronos as a cognitive model where authors used the concept of spike neural networks in the machine to analyze the data in the artificial mind. They also used the Quantum Neuro-Computing Framework concept where the consciousness is merged for them based on several conscious and unconscious parameters such as motivation, emotions, and synchronization circadian clock.

In another study [21], the authors discussed that consciousness does not adopt for intelligence phenomena because it is used for internal behavior. Furthermore, the authors discussed that consciousness intelligence is one of the outputs for the external behavior of an agent. The most important cognitive factors are memory, metacognition, emotions, perception, behavioral variations, and conceptual learning [22]. Also, for the cognitive and functional correlations; learning defines the agency which is related to the cognitive agent's learning ability for information patterns extraction from the external environment [23]. In another study [24], decision-making and emotions emphasized biologically plausible integration where the neural models process it rather than drift–diffusion of decision-making. For security purposes, the Edmund is used for emotions in their simulation model.

3 Artificial general intelligence-based rational behavior detection agent

An AI system aims to simulate human thoughts and is used to run the artificial cognitive processes for computer systems to build cognitive models. Cognitive science is used to develop the capabilities of thinking, learning, and decision-making in an agent [25]. In [26], authors discussed that cognitive science may provide human-like cognition such as the ability to think, learn by examples, doubt, act, see, and speak to the machine in a cognitive agent [27]. The cognitive agent may have a deficiency of rationality and weakness in managing the behavioral changes. In a cognitive agent, human-like capabilities can play an important role to acquire new skills and knowledge for analyzing the behavior of the other agents. Due to these deficiencies, a cognitive agent is not able to make its own decision in critical situations.

Figure 1 presents an overview of the Behavior Detection System (BDS) that is like a human brain for analyzing and

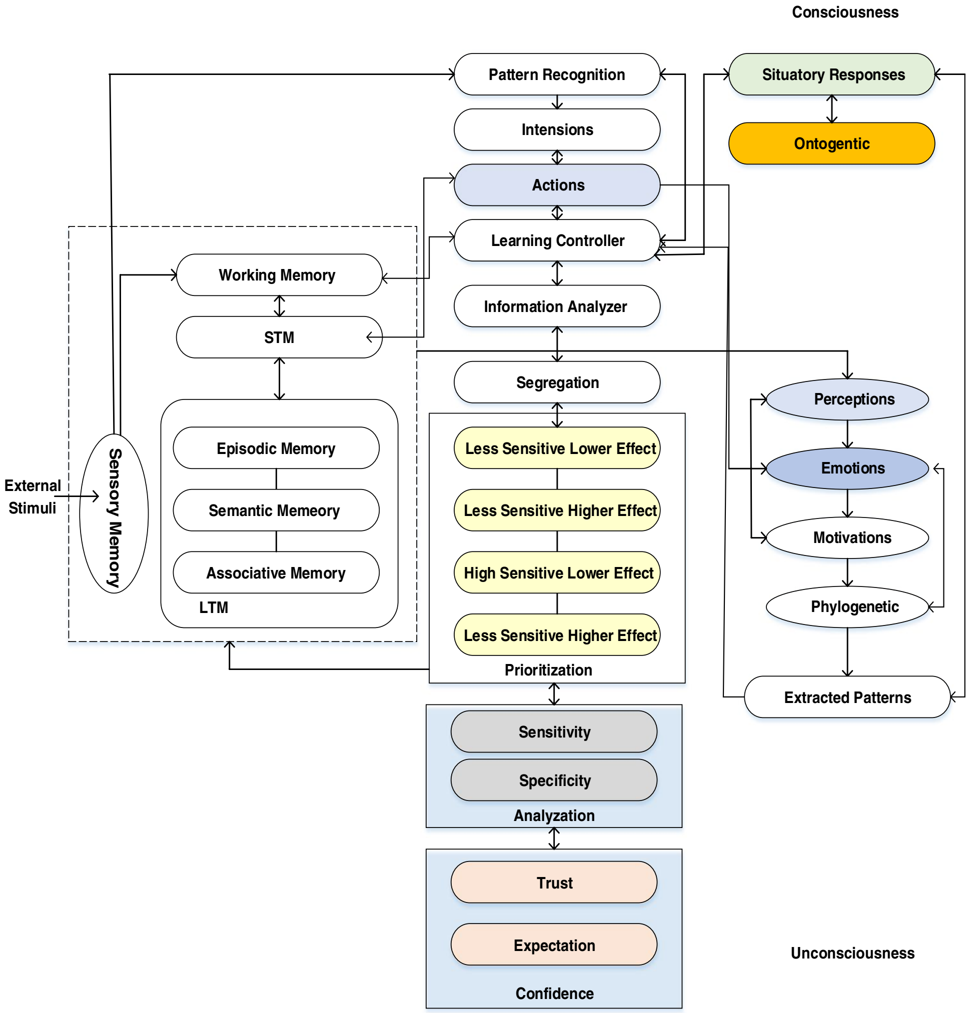


Fig. 1 Behavior detection system

sharing sensitive information with others using cognitive science. In this system, cognitive science plays a vital role in the selection of relevant information for security purposes using some cognitive correlates like intention, perception, motivation, and emotions. After achieving rationality, the BDS gains the capability to perform different cognitive processes such as perception, reasoning, decision-making, problem-solving, and taking action. To perform these processes, BDS contains main components such as memory, consciousness, unconsciousness, and security. All these components communicate with each other to protect sensitive information before sharing these components as discussed in the next sub-sections.

3.1 Memory

In BDS, memory is an essential part of human life. Without experience, a human cannot operate his/her activities in the present nor think about the future. A human would not be able to remember what they did yesterday, what they have done today, or what they plan to do tomorrow. Without memory, a human could not learn anything. Memory is involved in processing a vast amount of information in the forms of images, sounds, or meanings, etc. Memory consists of sub-memories such as sensory memory, working memory, short-term memory (STM), long-term memory (LTM), episodic memory, semantic memory, and associative memory. Sensory memory is essential to receive and process the information received from the environment. It is responsible for sharing the received information to short-term memory via working memory and for sharing the information to the data acquisition module for converting the information in the computer understandable form [28]. Working memory is used to process all activities performed in the memory that is to share the information received from sensory memory and share it with the STM.

Short term memory (STM) is used to rehearse the processed information in the memory to the conscious module and unprocessed information to the unconscious module for taking an action. It holds the information for a short time before sharing it with in the next sub-sections. LTM is used to store the information for a long time and process the information received from the external environment. LTM is based on three sub-memories that are episodic memory, semantic memory, and associative memory. Episodic memory is responsible to maintain the information about different events that occurred in the external environment such as time. Semantic memory is responsible to generate semantic or similar patterns such as facts, things of the rehearsed information received from the external environment. Semantics are the patterns that we know already but we cannot recall them. Semantic memory is responsible to elaborate on the asemantic information and create the associations of the elaborated information to generate more semantics.

3.2 Consciousness and unconsciousness

Human consciousness refers to an amazing wonder and gift for humankind. It integrates cognitive correlates such as intention, motivation, perception, and emotions for analyzing the information patterns based on different events that occurred in the external environment. Consciousness is used for decision-making to gain experience by using thinking and learning processes. Also, consciousness describes real-time information that is related to the emotional status of a human and his relationship to the external environment. In the BDS, consciousness receives the processed information from STM and generates situation responses for analyzing the agent's behavior to share the information. In consciousness, ontogenetic is used for decision-making for receiving, analyzing the rehearsed information patterns from memory, and generating the stimulatory responses using explicit learning.

On the other hand, unconsciousness is required to process the information patterns that are unable to process through consciousness. In unconsciousness, phylogenetic is responsible to perform cognitive processes of experiences using implicit knowledge without any conscious knowledge. Phylogenetic can recognize the particular occurrences of events in the external environment. In phylogenetic, knowledge plays an important role in generating the desired patterns that require generating situation responses in consciousness. In unconsciousness, intention, perception, motivation, and emotions play an important role to analyze and process the unprocessed information patterns coming from memory. In unconsciousness, if negative emotions are generated, then the BDS behavior will be different as compared to positive emotions. Similarly, if motivations to protect sensitive information were high, the probabilities of information sharing would be high. In an agency, learning plays an important role to act more efficiently.

3.3 Cognitive correlates

In an agency, learning is used to evaluate the reliability of action. Learning enables an agent to perceive information from the external environment, adopt it, and take an action based on some cognitive correlates such as intention, perception, motivation, and emotions. In an agency, the intention is required to understand the good or bad behavior of an agent after receiving the information patterns about an event that occurred in the external environment. Intention also requires differentiating between conscious and unconscious behavior. Perception is a major part of a cognitive agent that is required to understand behavior. It is a

Table 1 Rational behavior

Rule #	Motivation	Emotions	Behavior
R1	No	No	No
R2	No	Less	Disappointment
R3	No	Average	Disappointment
R4	No	High	Rational
R5	Less	No	No
R6	Less	Less	Disappointment
R7	Less	Average	Disappointment
R8	Less	High	Rational
R9	Average	No	No
R10	Average	Less	Disappointment
R11	Average	Average	Normal
R12	Average	High	Rational
R13	High	No	No
R14	High	Less	Disappointment
R15	High	Average	Normal
R16	High	High	Normal

mechanism with which a cognitive agent evaluates the information patterns, which in turn, determines the behavioral response [29]. Perception requires combining to extract the relevant information from the information patterns about the events that occurred in the external environment. It compares the extracted information patterns with the information patterns already stored in the memory. Perception also requires generating the intention of an agent for taking an action. Motivation refers to internal and external factors. In the proposed information-protecting agent, the phylogenetic module extracts the relevant emotional information patterns by using the motivation module. An optimized algorithm is used in the motivation module. The emotions are generated by using the experience of consciousness. The primary emotions occurred whenever any event occurs and are noticed from the external environment. The secondary emotion occurred for the response of primary emotion. The state of emotion will be negative or positive depending upon human moods such as personality, disposition, temperature, and motivation.

Cognition is one of the significant aspects of emotion and is based on human feelings. The emotions are related to subject experience, behavior change, cognitive processes, and expressive behavior. In unconsciousness, the emotions receive priority to extract control over the processing of unrehearsed information. Cognitive science plays a vital role in keeping emotionally distracting and intrusive emotions out of memory. Such emotions are problematic in a variety of disorders such as depression and anxiety [30]. If motivation is less than the emotions, then the behavior of BDS is rational up to when the level of emotions and motivation becomes equal. If the motivation level is higher than the emotions, then the behavior of the system will be disappointed [31]. In an agency, the cognitive parameters are similar to human cognitive parameters. For example, in an unconscious module, if negative emotions are generating, then the human decision power will be different as compared to positive emotions. Similarly, in an unconscious module, if motivations are high to secure information, the possibilities of information sharing would be high. After achieving rationality, an agent becomes capable to interact with the external environment and can perform the following cognitive processes such as perception, reasoning, decision making, problem-solving and action using the cognitive correlates emotions, motivation, and implicit and explicit learning.

In an agency, the intention is required to understand the good or bad behavior of an agent after receiving the information patterns about an event that occurred in the external environment. Intention also requires differentiating between conscious and unconscious behavior. Perception is a major part of a cognitive agent that is required to understand behavior. It is a mechanism with which a cognitive agent evaluates the information patterns, which in turn, determines the behavioral response. Perception requires combining to extract the relevant information from the information patterns about the events that occurred in the

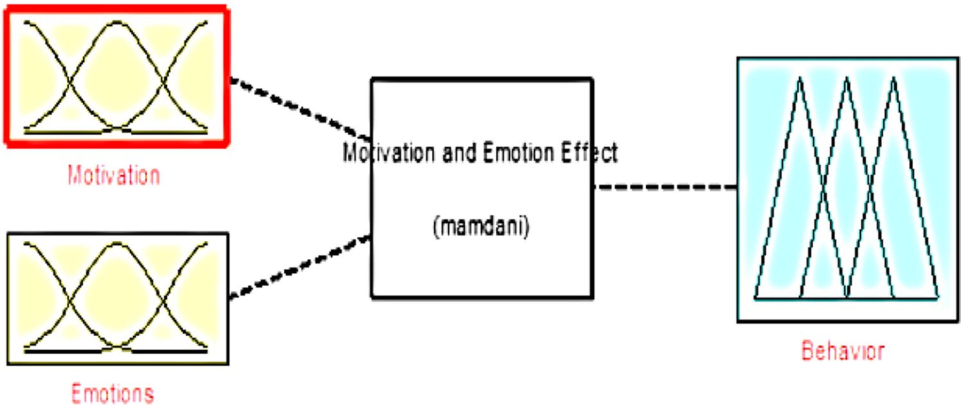


Fig. 2 Motivation and emotion effect

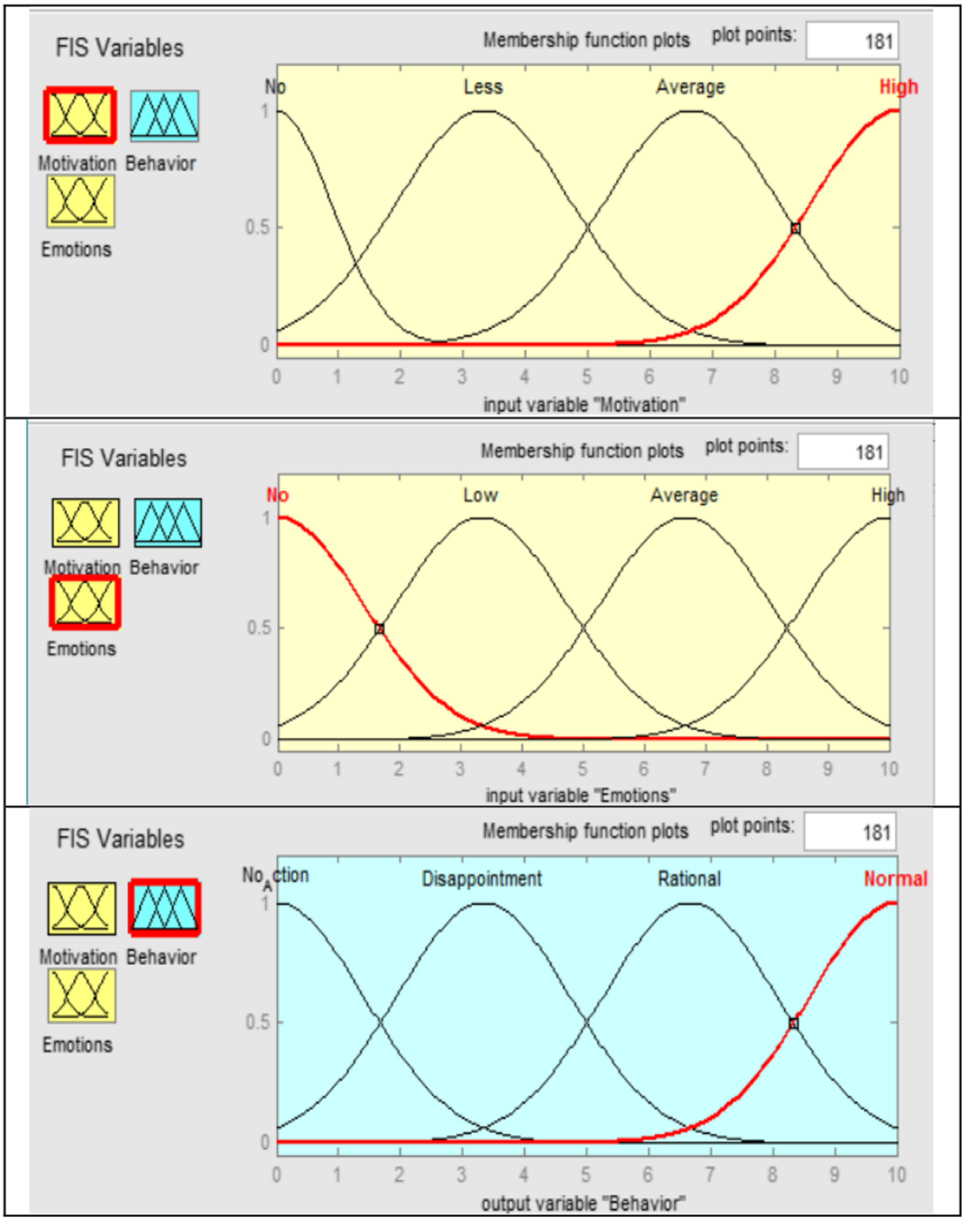
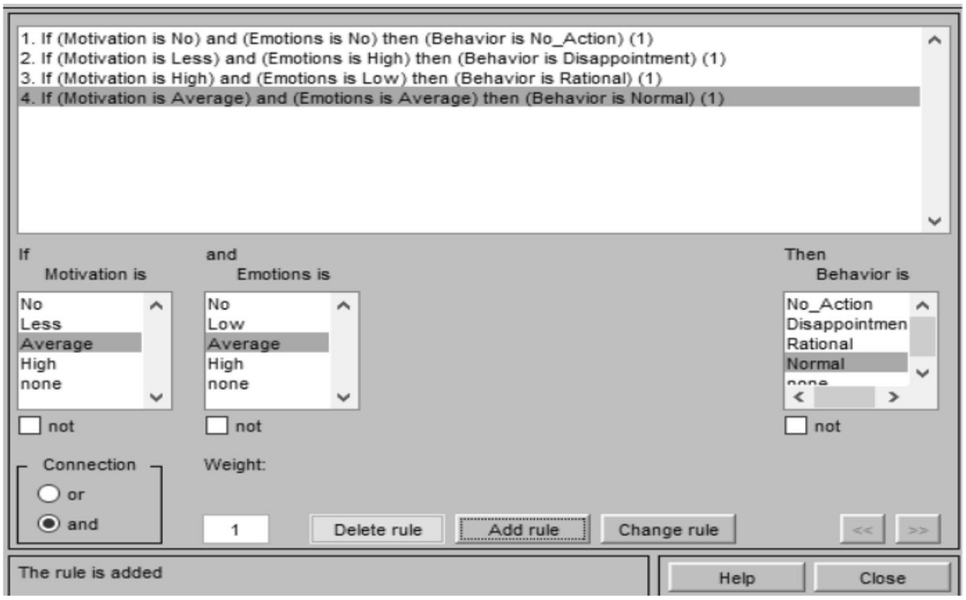


Fig. 3 **a** Motivation Membership, **b** Emotions Membership, and **c** Behavior Membership

external environment. It compares the extracted information patterns with the information patterns already stored in the memory. Perception also requires generating the intention of an agent for taking an action. Motivation is the internal and external factors and people to be continuously interested to communicate sensitiveinformation. In the proposed information-protecting agent, the phylogenetic module extracts the relevant emotional information patterns through the motivation module. The motivation module uses an optimized algorithm with a person's retrieval motivation. In an agency, emotions are generated based on the experience of the consciousness. Primary emotions occur when an event occurs in the external environment and secondary emotions occur in the response of primary emotions. Emotions may be positive or negative such as mood, temperature, personality, disposition, and motivation. Cognition is an important aspect of emotion. Emotions are the feelings of human behavior. Emotions are generated due to motivation either positive or negative. Emotions are based on subjective experience, cognitive processes, expressive behavior, and behavior changes.

Fig. 4 Rules defined for agent's behavior



1. If (Motivation is No) and (Emotions is No) then (Behavior is No_Action) (1)
2. If (Motivation is Less) and (Emotions is High) then (Behavior is Disappointment) (1)
3. If (Motivation is High) and (Emotions is Low) then (Behavior is Rational) (1)
4. If (Motivation is Average) and (Emotions is Average) then (Behavior is Normal) (1)

If Motivation is: No, Less, Average, High, none
□ not

and Emotions is: No, Low, Average, High, none
□ not

Then Behavior is: No_Action, Disappointmen, Rational, Normal, none
□ not

Connection: ○ or ● and

Weight: 1

The rule is added

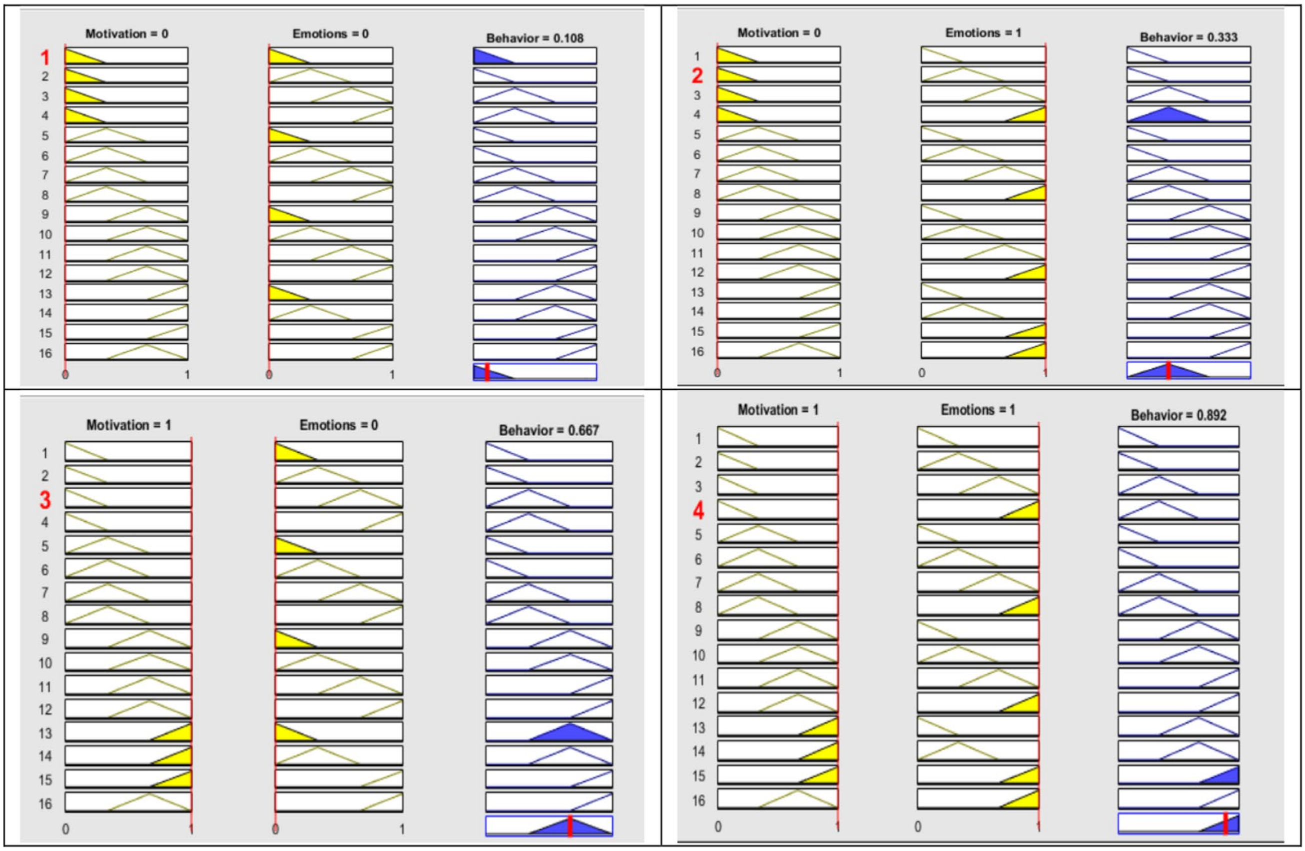


Fig. 5 Behavior of agents. **a** Behavior of agent when no motivation, no emotions, **b** Behavior of agent when no motivation, but there are some emotions, **c** Behavior of agent when there is some motivation, but there are no emotions, and **d** Behavior of agent when there is some motivation as well as some emotions

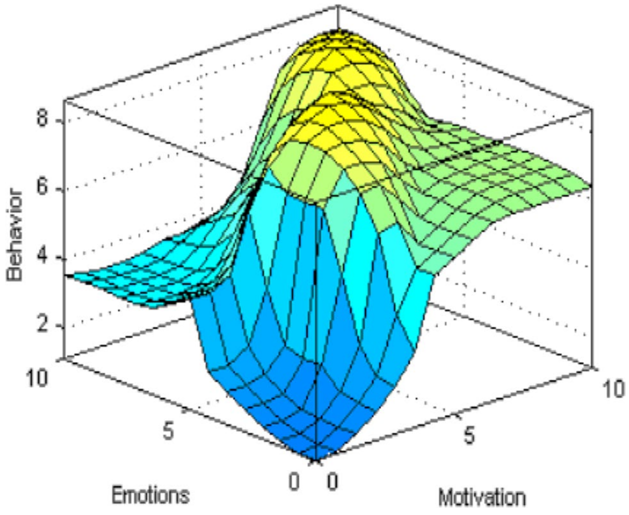


Fig. 6 Motivation, emotions impact on cognitive agent's behavior

In unconsciousness, emotions receive priority to extract control over the processing of unrehearsed information.

3.4 Security component

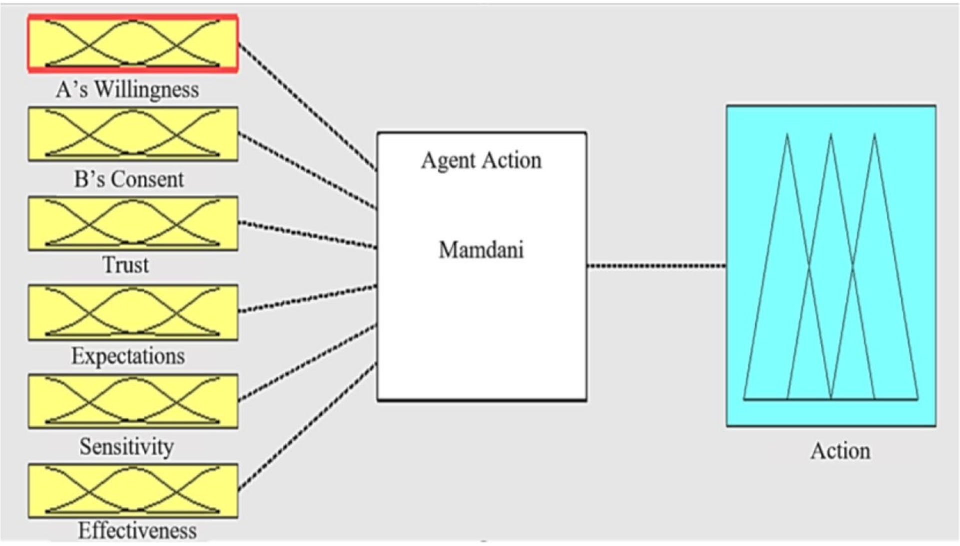
In the proposed system, when a new information pattern about some events that occurred in the external environment arrives in the segregation module d[i], it first checks the receiving pattern that is suitable to share with the remote agent in the system or not. If it considers the information suitable to share, then it checks the sensitivity level of the received information pattern P[i] assigned to it. In the segregation module, the sensitivity level of the information pattern is checked against the minimum sensitivity level assumed which is a threshold value (α), and if the sensitivity level is less than the threshold level, then it is considered to be not shareable to the remote agent, and instead, it is shared to the memory for later use. If the sensitivity level of the information pattern is less than the threshold value, then there are two considerations:

1. A new information pattern with higher sensitivity, i.e., the information pattern with sensitivity P[α + 1] is selected for sharing it with the remote agent.
2. The process waiting time (tw) at the segregation module and information sharing time (td) from the segregation module of information pattern P[i] to the new remote agent is calculated. The new information pattern is the first pattern having the sensitivity level above the threshold value, i.e., information pattern with sensitivity level P[α + 1]. The segregation module is efficient in executing the new information pattern 49 because its priority is higher than the threshold value (α). If the information pattern P is less sensitive, then required information needs to be transmitted to the remote agent with a sensitivity level [α + 1] which increases the information transmission time depending upon the no. of patterns covered to transmit to the desired agent.

Now even if the information is less sensitive, but if the segregation module is overloaded, it may take more time to share that information with the desired agent in the system. Such information may have to wait for a long time in the waiting queue of the segregation module. So, a threshold value level is declared based on the fact that for how long new information should remain in the waiting queue, i.e., called β.

If tw > β and if tw > td, that information is shared to the remote agent in the system else information is kept in the waiting queue in the segregation module else information is kept in waiting for queue in the long term memory for later on

Fig. 7 Cognitive agent's decision-making variables



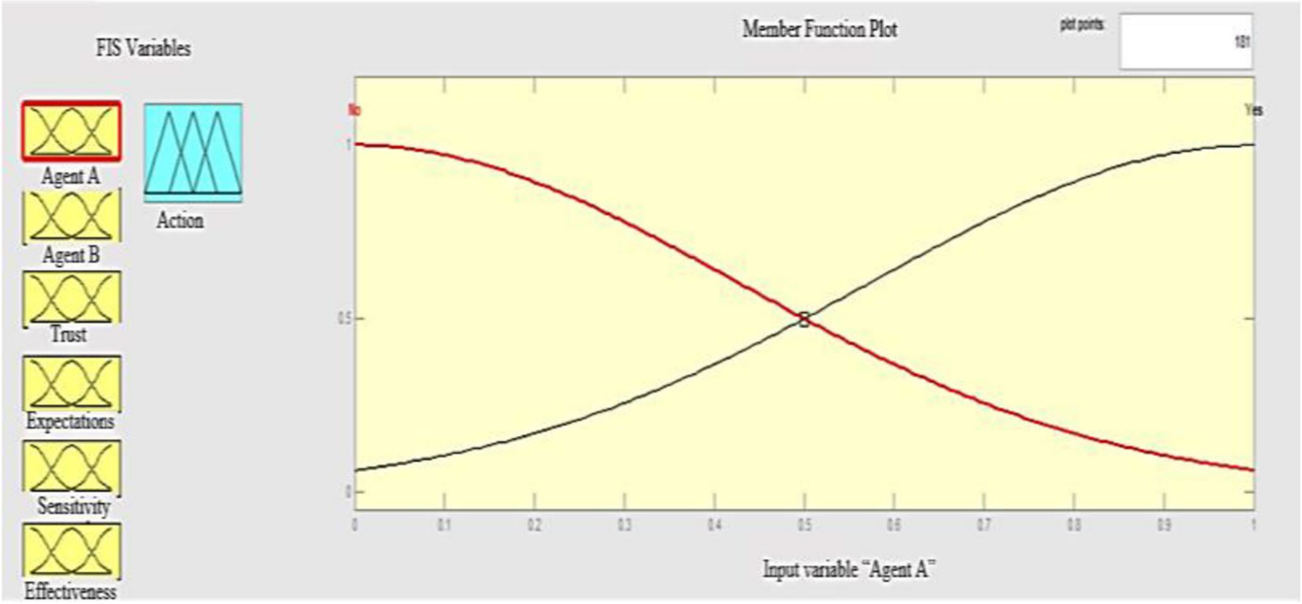


Fig. 8 Agent-A's membership functions

use. If the waiting time (tw) at the segregation module exceeds P[i], then it is better to share the information to the remote agent of high sensitivity with the condition that information sharing time (td) to the remote agent is less than waiting time at segregation module; so here, two conditions are checked.

i. Waiting time at segregation module is checked against a threshold value β, so that a process does not block for longer and if the waiting time for processing information at segregation module is greater than threshold value β, then waiting time is checked against information sharing time to the other agent.
ii. If the waiting time is less than the information sharing time, the process is still made to wait in the waiting queue at the segregation module but if the information sharing time is less than waiting time, then

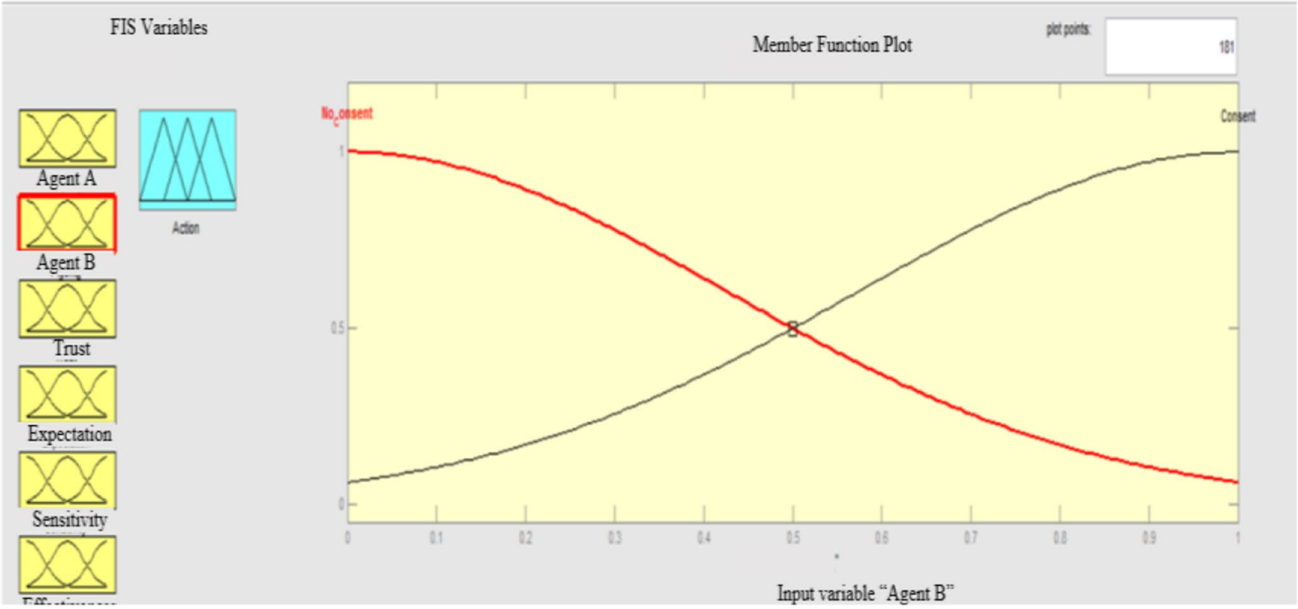


Fig. 9 Agent-B's membership functions

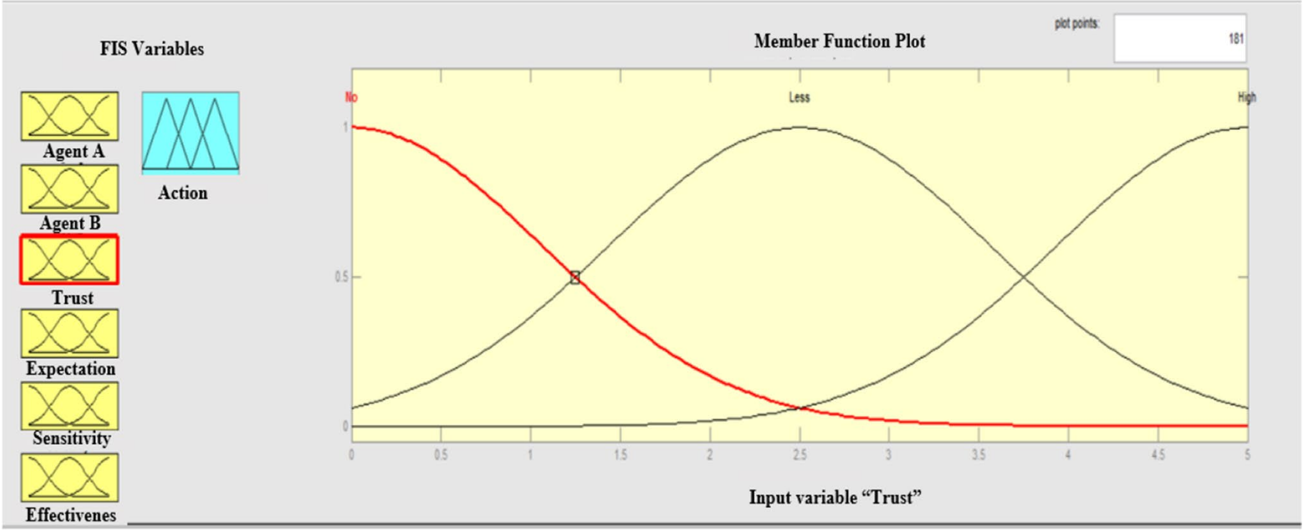


Fig. 10 Agent-A trust on agent-B membership functions

information is shared from the segregation module to the higher priority chosen agent. The algorithm works based on mathematical complexities which are as follows:

```
$L$= Information patterns received at segregation module
$td$= information sharing time
$t[i]$= time is taken by the segregation module for processing i patterns.
$tw$ = waiting time for sharing information.
$n$ = No. of information patterns
$Tpt$= Token processing time taken by the segregation module
$Tpt$=$(n*td+tp[i])$, total processing time taken by the segregation module.
$td$=0 data transmission time=0, because no data is transmitted through the segregation module.
$Tpt$=$(n*td+tp[i]+tw)$, where waiting time is concerned.
$(\propto)$=where α is the threshold level.
$(\propto+1)$= high sensitive information
In the case of high sensitivity, segregation module, waiting time is 0, because enough memory is available of new pattern sharing.
$Tpt$=$(0+tp[i]+tw)$
$Tpt$=$(0*td+tp[i]+0)$
$Tpt$=$(tp[i])$
If the information is less sensitive, then the waiting time needs to be taken into consideration.
$Tpt$=$(0+tp[i]+tw)$
$Tpt$=$(tp[i]+tw)$
$\beta$= Threshold value to decide how long a new information pattern have to wait to process
If $tw>\beta$ then
If $tw>td$ then the information will be shared to the remote agent
    Else
Information is kept in a waiting queue in the segregation module
    Else
Information will be processed to memory for reprocessing whenever is required.
At remote agent, tw=0 then Tpt = L(ntd +Tp[i]+0)
```

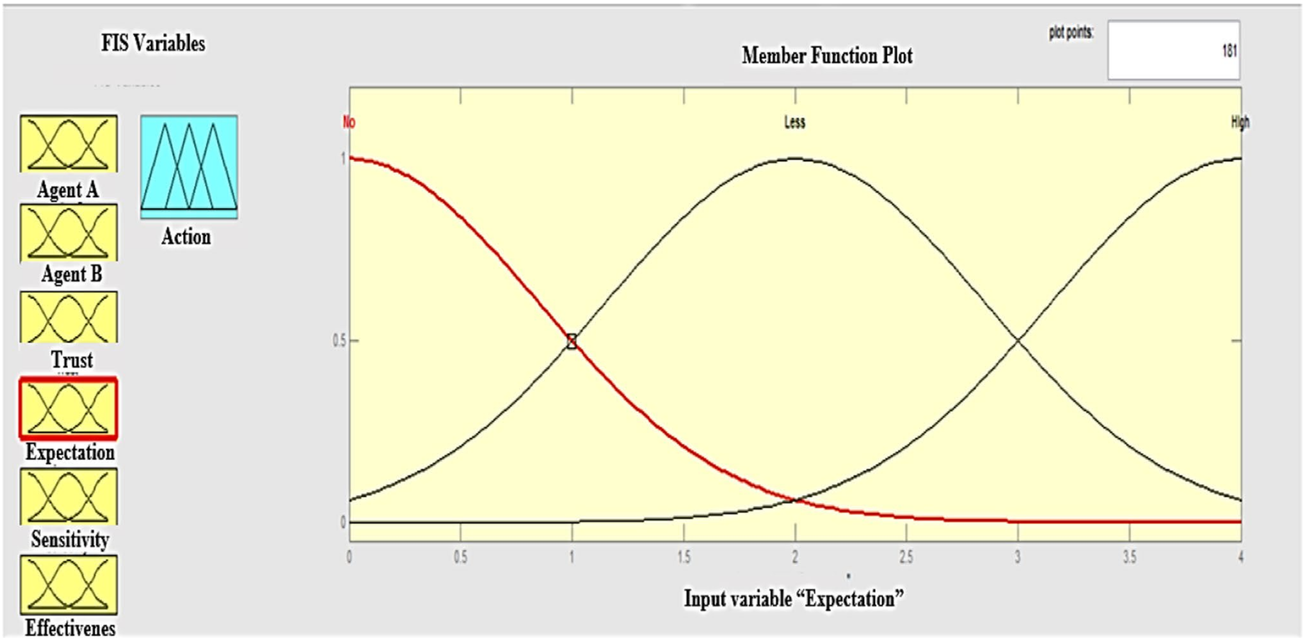


Fig. 11 Agent-A expectation on Agent-B membership functions

4 Simulation of rational behavior

The fuzzy logic techniques are comparatively simpler as it requires only some linguistic rules for information protection. In this paper, we have used fuzzy logic techniques for analyzing the behavior of cognitive agents for taking an action, i.e., to share sensitive information with other agents after analyzing the sensitivity of the information. First, to analyze the rational behavior based on motivation and emotions, we have generated 16 rules that are given below in Table 1:

In Fig. 2, for analyzing the rational behavior of a cognitive agent, we have taken two input variables including

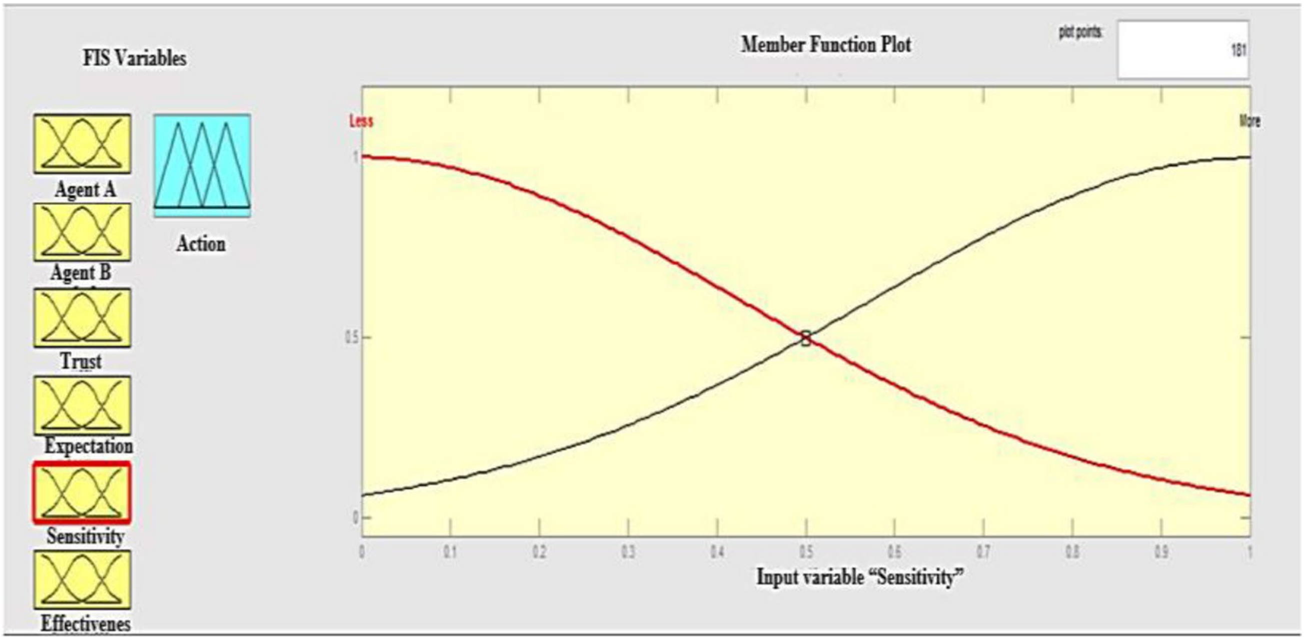


Fig. 12 Sensitivity of information membership functions, i.e., less or more

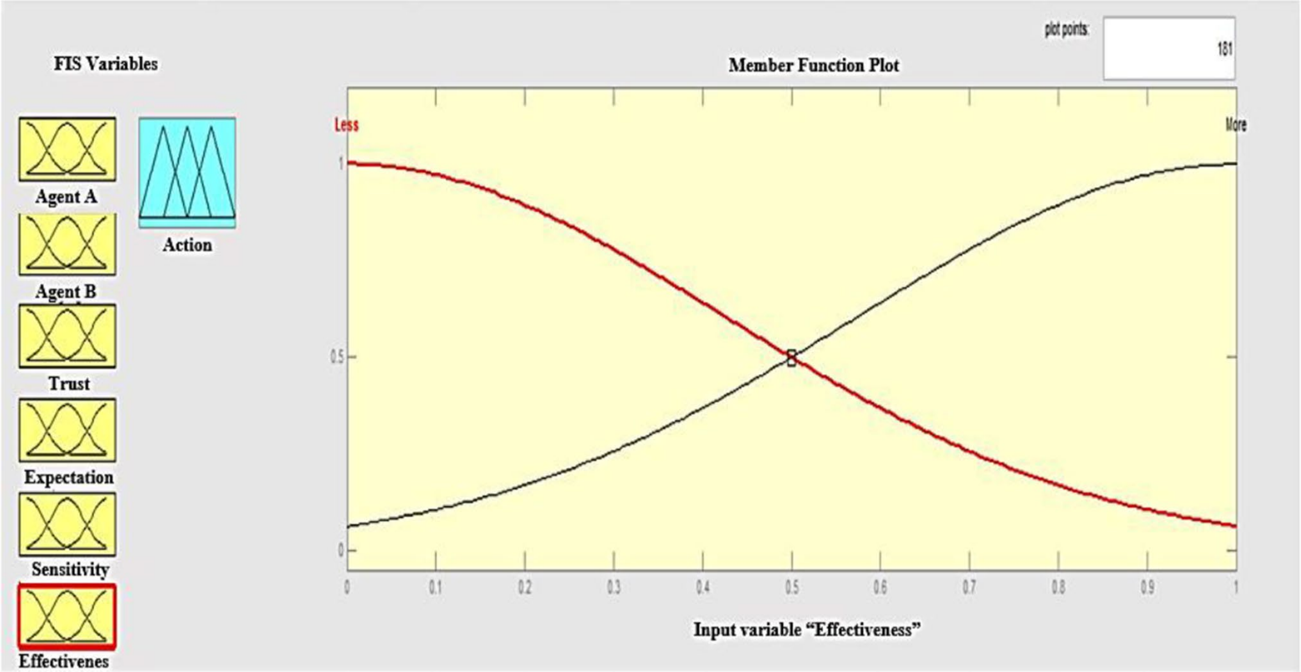


Fig. 13 Effectiveness of information membership functions, i.e., less or more

Motivation and Emotion, and one output variable including Behavior using the Mamdani model. In the next setup, we have taken four membership functions of MOTIVATION including No, Less, Average, and High. Then, we have taken four membership functions of EMOTIONS including No, Less, Average, and High. Afterward, we have taken four membership functions of BEHAVIOR, i.e., No, Disappointment, Rational, and Normal. These four setups are shown in Fig. 3.

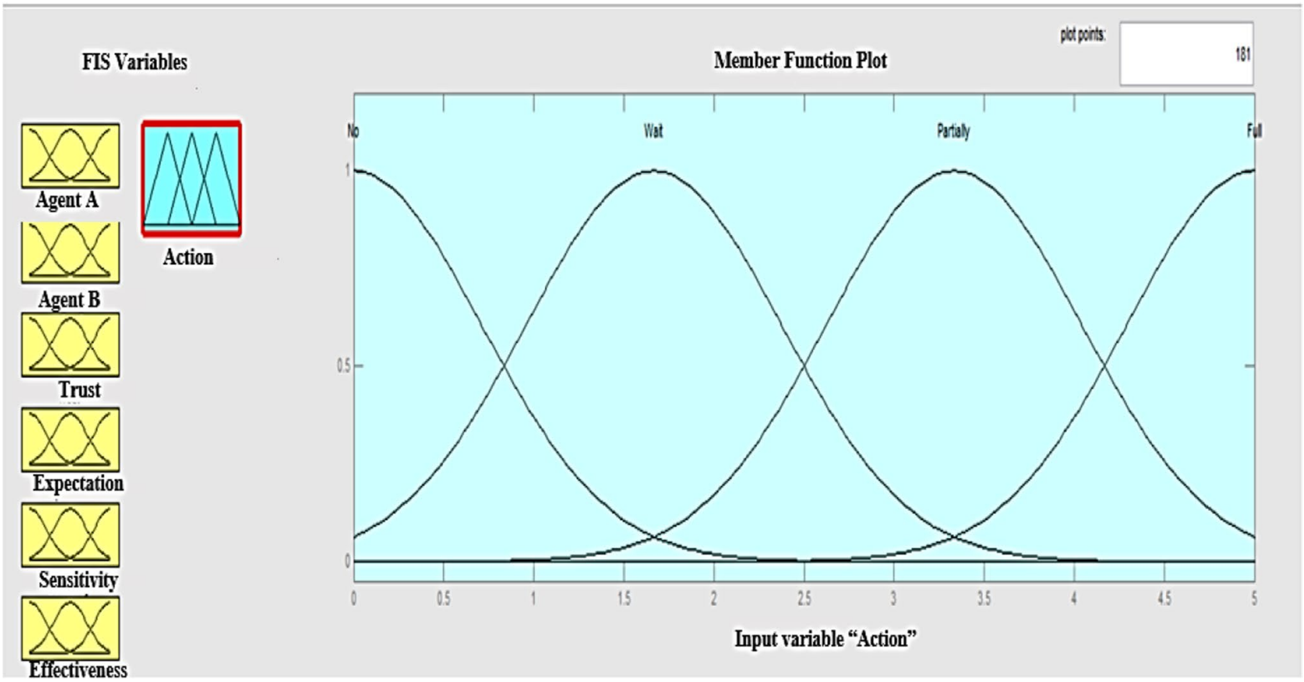


Fig. 14 Agent-A's action membership functions

Table 2 Action taken by Agent–A

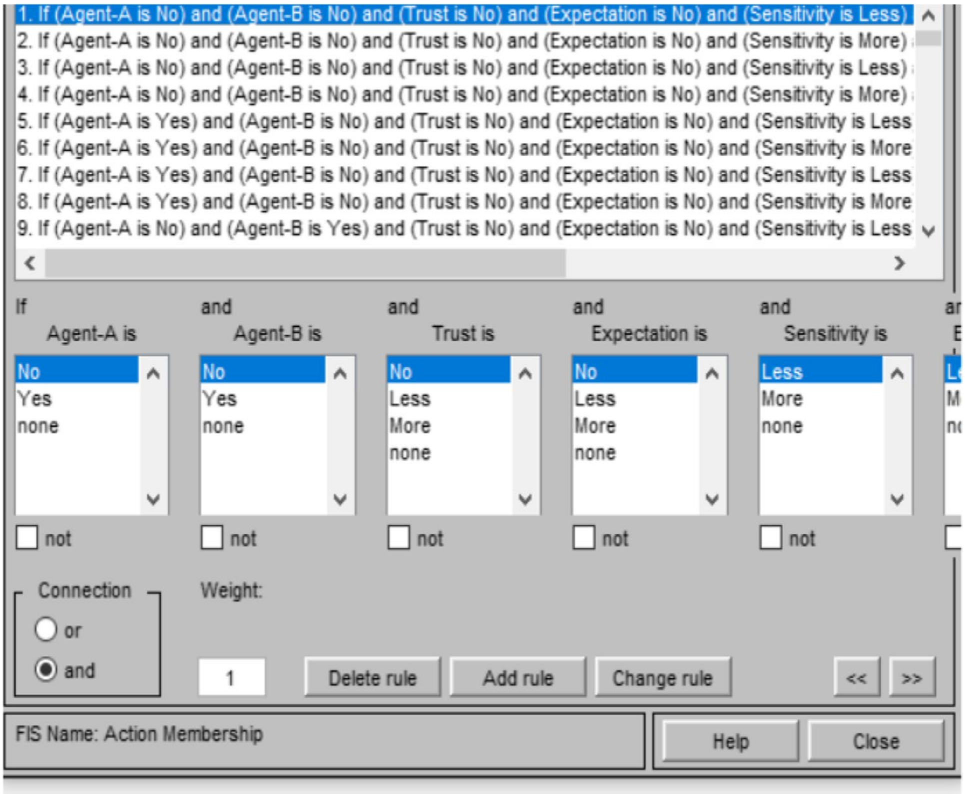
Rule No	Agent-A	Agent-B	Trust	Expectation	Sensitivity	Effectiveness	Action
R1	No	No	No	No	Less	Less	No
R2	No	No	No	No	More	Less	No
R3	No	No	No	No	Less	More	No
R4	No	No	No	No	More	More	No
R5	Yes	No	No	No	Less	Less	No
R6	Yes	No	No	No	More	Less	No
R7	Yes	No	No	No	Less	More	No
R8	Yes	No	No	No	More	More	No
R9	No	Yes	No	No	Less	Less	No
R10	No	Yes	No	No	More	Less	No
R11	No	Yes	No	No	Less	More	No
R12	No	Yes	No	No	More	More	No
R13	Yes	Yes	No	No	Less	Less	No
R14	Yes	Yes	No	No	More	Less	No
R15	Yes	Yes	No	No	Less	More	No
R16	Yes	Yes	No	No	More	More	No
R17	No	No	No	Less	Less	Less	No
R18	No	No	No	Less	More	Less	No
R19	No	No	No	Less	Less	More	No
R20	No	No	No	Less	More	More	No
R21	Yes	No	No	Less	Less	Less	No
R22	Yes	No	No	Less	More	Less	No
R23	Yes	No	No	Less	Less	More	No
R24	Yes	No	No	Less	More	More	No
R25	No	Yes	No	Less	Less	Less	No
R26	No	Yes	No	Less	More	Less	No
R27	No	Yes	No	Less	Less	More	No
R28	No	Yes	No	Less	More	More	No
R29	Yes	Yes	No	Less	Less	Less	No
R30	Yes	Yes	No	Less	More	Less	No
R31	Yes	Yes	No	Less	Less	More	No
R32	Yes	Yes	No	Less	More	More	No
R33	No	No	No	More	Less	Less	No
R34	No	No	No	More	More	Less	No
R35	No	No	No	More	Less	More	No
R36	No	No	No	More	More	More	No
R37	Yes	No	No	More	Less	Less	No
R38	Yes	No	No	More	More	Less	No
R39	Yes	No	No	More	Less	More	No
R40	Yes	No	No	More	More	More	No
R41	No	Yes	No	More	Less	Less	No
R42	No	Yes	No	More	More	Less	No
R43	No	Yes	No	More	Less	More	No
R44	No	Yes	No	More	More	More	No
R45	Yes	Yes	No	More	Less	Less	No
R46	Yes	Yes	No	More	More	Less	No
R47	Yes	Yes	No	More	Less	More	No
R48	Yes	Yes	No	More	More	More	No
R49	No	No	Less	No	Less	Less	No
R50	No	No	Less	No	More	Less	No
R51	No	No	Less	No	Less	More	No

Table 2 (continued)

Rule No	Agent-A	Agent-B	Trust	Expectation	Sensitivity	Effectiveness	Action
R52	No	No	Less	No	More	More	No
R53	Yes	No	Less	No	Less	Less	No
R54	Yes	No	Less	No	More	Less	No
R55	Yes	No	Less	No	Less	More	No
R56	Yes	No	Less	No	More	More	No
R57	No	Yes	Less	No	Less	Less	No
R58	No	Yes	Less	No	More	Less	No
R59	No	Yes	Less	No	Less	More	No
R60	No	Yes	Less	No	More	More	No
R61	Yes	Yes	Less	No	Less	Less	No
R62	Yes	Yes	Less	No	More	Less	No
R63	Yes	Yes	Less	No	Less	More	No
R64	Yes	Yes	Less	No	More	More	No
R65	No	No	Less	Less	Less	Less	No
R66	No	No	Less	Less	More	Less	No
R67	No	No	Less	Less	Less	More	No
R68	No	No	Less	Less	More	More	No
R69	Yes	No	Less	Less	Less	Less	No
R70	Yes	No	Less	Less	More	Less	Less
R71	Yes	No	Less	Less	Less	More	No
R72	Yes	No	Less	Less	More	More	Less
R73	No	Yes	Less	Less	Less	Less	No
R74	No	Yes	Less	Less	More	Less	No
R75	No	Yes	Less	Less	Less	More	No
R76	No	Yes	Less	Less	More	More	No
R77	Yes	Yes	Less	Less	Less	Less	No
R78	Yes	Yes	Less	Less	More	Less	Partially
R79	Yes	Yes	Less	Less	Less	More	No
R80	Yes	Yes	Less	Less	More	More	Partially
R81	No	No	Less	More	Less	Less	No
R82	No	No	Less	More	More	Less	No
R83	No	No	Less	More	Less	More	No
R84	No	No	Less	More	More	More	No
R85	Yes	No	Less	More	Less	Less	No
R86	Yes	No	Less	More	More	Less	Less
R87	Yes	No	Less	More	Less	More	No
R88	Yes	No	Less	More	More	More	Less
R89	No	Yes	Less	More	Less	Less	No
R90	No	Yes	Less	More	More	Less	No
R91	No	Yes	Less	More	Less	More	No
R92	No	Yes	Less	More	More	More	No
R93	Yes	Yes	Less	More	Less	Less	No
R94	Yes	Yes	Less	More	More	Less	Partially
R95	Yes	Yes	Less	More	Less	More	No
R96	Yes	Yes	Less	More	More	More	Partially
R97	No	No	More	No	Less	Less	No
R98	No	No	More	No	More	Less	No
R99	No	No	More	No	Less	More	No
R100	No	No	More	No	More	More	No
R101	Yes	No	More	No	Less	Less	No
R102	Yes	No	More	No	More	Less	No

Table 2 (continued)

Rule No	Agent-A	Agent-B	Trust	Expectation	Sensitivity	Effectiveness	Action
R103	Yes	No	More	No	Less	More	No
R104	Yes	No	More	No	More	More	No
R105	No	Yes	More	No	Less	Less	No
R106	No	Yes	More	No	More	Less	No
R107	No	Yes	More	No	Less	More	No
R108	No	Yes	More	No	More	More	No
R109	Yes	Yes	More	No	Less	Less	No
R110	Yes	Yes	More	No	More	Less	No
R111	Yes	Yes	More	No	Less	More	No
R112	Yes	Yes	More	No	More	More	No
R113	No	No	More	Less	Less	Less	No
R114	No	No	More	Less	More	Less	No
R115	No	No	More	Less	Less	More	No
R116	No	No	More	Less	More	More	No
R117	Yes	No	More	Less	Less	Less	No
R118	Yes	No	More	Less	More	Less	Less
R119	Yes	No	More	Less	Less	More	No
R120	Yes	No	More	Less	More	More	Less
R121	No	Yes	More	Less	Less	Less	No
R122	No	Yes	More	Less	More	Less	No
R123	No	Yes	More	Less	Less	More	No
R124	No	Yes	More	Less	More	More	No
R125	Yes	Yes	More	Less	Less	Less	No
R126	Yes	Yes	More	Less	More	Less	Partially
R127	Yes	Yes	More	Less	Less	More	No
R128	Yes	Yes	More	Less	More	More	Partially
R129	No	No	More	More	Less	Less	No
R130	No	No	More	More	More	Less	No
R131	No	No	More	More	Less	More	No
R132	No	No	More	More	More	More	No
R133	Yes	No	More	More	Less	Less	No
R134	Yes	No	More	More	More	Less	Less
R135	Yes	No	More	More	Less	More	No
R136	Yes	No	More	More	More	More	Less
R137	No	Yes	More	More	Less	Less	No
R138	No	Yes	More	More	More	Less	No
R139	No	Yes	More	More	Less	More	No
R140	No	Yes	More	More	More	More	No
R141	Yes	Yes	More	More	Less	Less	No
R142	Yes	Yes	More	More	More	Less	Full
R143	Yes	Yes	More	More	Less	More	No
R144	Yes	Yes	More	More	More	More	Full



1. If (Agent-A is No) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is Less)
2. If (Agent-A is No) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is More)
3. If (Agent-A is No) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is Less)
4. If (Agent-A is No) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is More)
5. If (Agent-A is Yes) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is Less
6. If (Agent-A is Yes) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is More
7. If (Agent-A is Yes) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is Less
8. If (Agent-A is Yes) and (Agent-B is No) and (Trust is No) and (Expectation is No) and (Sensitivity is More
9. If (Agent-A is No) and (Agent-B is Yes) and (Trust is No) and (Expectation is No) and (Sensitivity is Less

If Agent-A is: No
and Agent-B is: No
and Trust is: No
and Expectation is: No
and Sensitivity is: Less

Connection: ○ or ● and

Weight: 1

FIS Name: Action Membership

Fig. 15 Rules editors for action taken

In Fig. 4, we have defined 16 rules for analyzing the agent's behavior based on motivation and emotional membership functions. We have also shown multiple behavior impacts with the changing of motivation and emotions (Figs. 5, 6).

In Fig. 7, for analyzing the behavior of a cognitive agent to take an action, i.e., whether to share sensitive information to other agencies, we have taken six input variables, i.e., Agent-A, Agent-B, Trust, Expectation, Sensitivity, and Effectiveness and one output variable, i.e., ACTION.

In Fig. 8, we have shown two membership functions of AGENT-A, i.e., No (Agent is not willing to share sensitive information) and Yes (Agent is willing to share sensitive information to Agent-B).

In Fig. 9, we have shown the consent membership functions of AGENT-B, i.e., No (agent is not willing to give consent to receive sensitive information from Agent-A) and Yes (means the agent is willing to give consent to receive information from Agent-A).

In Fig. 10, we have shown the TRUST level of Agent-A on Agent-B after it consented to receive the information, i.e., No, Less, or More.

In Fig. 11, we have shown the EXPECTATION level of Agent-A on Agent-B after it consented to receive the information and not further share the received sensitive information to any other agent, i.e., No, Less, or More.

In Fig. 12, we have shown two membership functions of about the SENSITIVITY level of the information to be shared from Agent-A to Agent-B, i.e., Less or more sensitive.

In Fig. 13, we have shown two membership functions of about the EFFECTIVENESS level of the information to be shared on the other agents in the system.

In Fig. 14, we have shown four membership functions of the action taken by Agent-A to share the information to Agent-B after his consent, checking the trust level and sensitivity level of information, i.e., No, Less, partially and full. After analyzing all these parameters, we have declared 144 rules for Agent-A to share sensitive information with Agent-B as shown in Table 2.

In Fig. 15, we have shown 144 rules based on six input variables, i.e., Agent-A willing to share the sensitive information, Agent-B consent to receive the sensitive information, level of trust and expectation on Agent-B, level of sensitivity of the information, and its effectiveness for taking an action for information sharing.

Figure 16 shows the behavior of Agent-A, when it is not willing to share the information, similarity, no of consent for Agent-B to recive the sensitive information which is less. The second graph shows the behavior of Agent-A, when it is ready to share the sensitive information to Agent-B, but there is no consent from Agent-B to receive any information for Agent-A. The third graph shows the behavior of Agent-A to

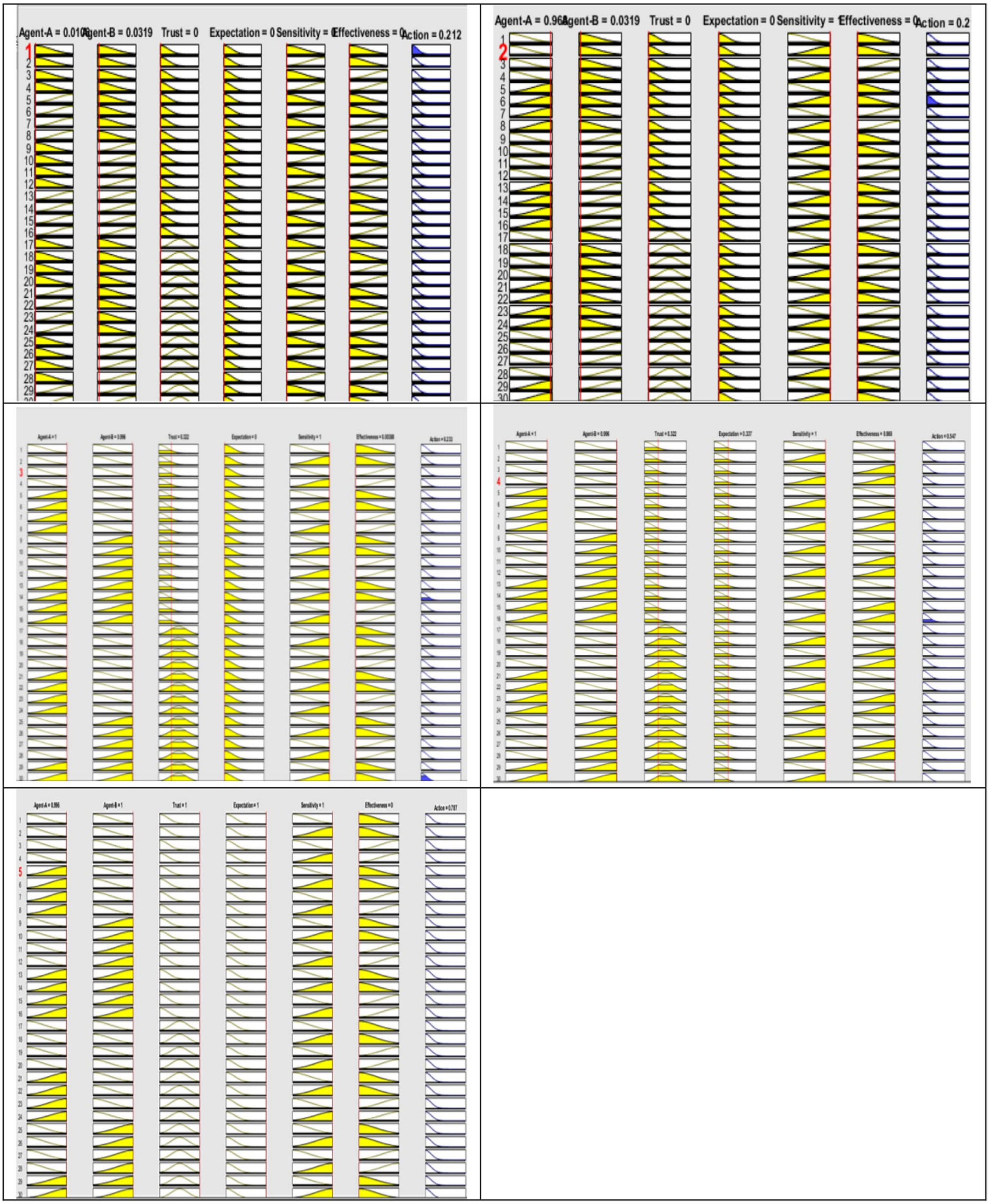


Fig. 16 **a** Agent-A decision when it is not willing to share the information, **b** Agent-A decision, when it is willing to share information, **c** Agent-A's behavior after some trust of Agent-B, **d** Agent-A behavior having some trust and expectation on Agent-B, **e** Agent-A behavior at more trust and more expectation on Agent-B

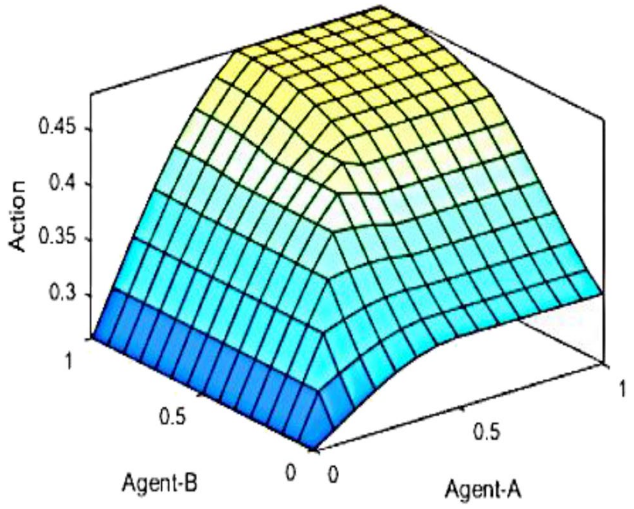


Fig. 17 Impact of Agent-A's willingness and Agent-B's consent for taking an action

share the part of sensitive information after having some trust in Agent-B. The fourth graph shows the behavior of Agent-A after having some trust and also some expectation that it will not further share with any other agent after receiving the sensitive information. The fifth graph shows the behavior of Agent-A regarding taking an action, i.e., either to share sensitive information or not and how much information is shared based on trust and expectation level on Agent-B.

Figure 17 shows the impact of action taken by Agent-A after the consent of Agent-B for sharing sensitive information.

Figure 18 shows the impact of Action taken by Agent-A based on trust and expectation level on Agent-B.

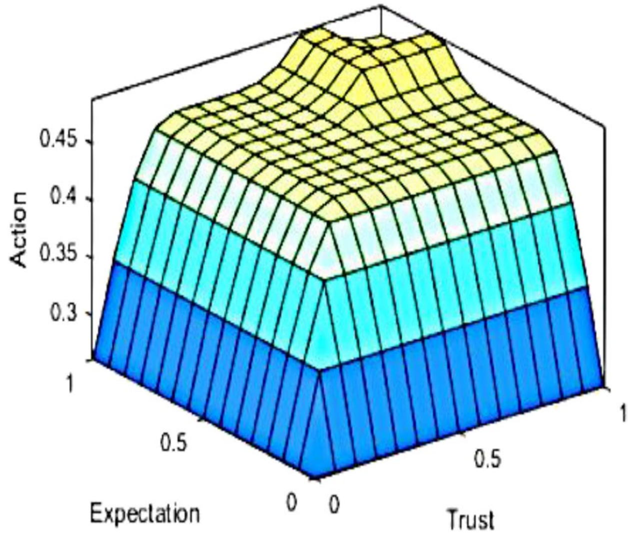


Fig. 18 Impact of trust and expectation on action

5 Conclusion

Various expert systems use several encryption techniques such as classical encryption and quantum encryption techniques for protecting imperative information. In this paper, we have proposed a cognitive information protection agent using artificial general intelligence, which is an advanced level of quantum encryption technique. Cognitive science has become the inspiration for artificial intelligence in terms of human-like rationality in decision-making and logical functionality. In our proposed agent, we have combined various cognitive factors such as intention, perception, motivation, and emotions to attain human-like information protection and manipulation capabilities because in cognitive science, the human mind does not encrypt the information, instead, it uses cognitive factors such as motivation, emotions, and learning for protecting the sensitive information before sharing it to other agents. In the cognitive information protection agent, the cognitive factors such as motivation, emotions, and categorization, trust, and expectation modules are communicated with each other for protecting the information before sharing it with other modules within the architecture. Our cognitive information protection agent is used for a positive association between extroversion and the level of sharing sensitive information for security purposes. The cognitive information protection agent categorizes the information into four categories based on its sensitivity and its effectiveness, i.e., less sensitive less effective, less sensitive more effective, more sensitive less effective, and more sensitive more effective before sharing it with other agents.

The cognitive information protection agent analyzes the trust and expectation level of the other agents with whom the information is going to be shared before sharing the sensitive information to these agents. An approach for behavior and actions taken by a cognitive agent analysis and classification of variables for behavior and actions based on fuzzy logic is found to be very efficient and effective under different rules. This technique can analyze not only the behavior and actions of a cognitive agent but can also give automatic memory protection in real-time. The system operation is fast, reliable, and secure. The proposed logic is simple since it requires only some linguistic rules. The results show that the proposed technique is simple, fast, and reliable and secure.

References

1. Abdel-Fattah AM, Besold TR, Gust H, Krumnack U, Schmidt M, Kuhnberger K-U, Wang P (2012) Rationality-guided AGI as cognitive systems. In: Proceedings of the Annual Meeting of the Cognitive Science Society 34(34)
2. Khan MM, Ghani I, Jeong SR, Ibrahim R, Qureshi KN (2016) Facebook's public social interaction utilization to assist recommendation across system domain. J Theoret Appl Inf Technol 88(3):392

3. Oravec J (2014) Expert systems and knowledge-based engineering (1984–1991): Implications for Instructional Systems Research. Int J Des Learn 5(2)
4. Qazi R, Qureshi KN, Bashir F, Islam NU, Iqbal S, Arshad A (2020) Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. J Ambient Intell Human Comput 12:547
5. Kaimal LB, Metkar AR, Rakesh G (2014) Self learning real time expert system. Int J Soft Comput Artif Intell Appl 3(2):13–25
6. Ahmad A, Paul A, Rathore MM (2016) An efficient divide-and-conquer approach for big data analytics in machine-to-machine communication. Neurocomputing 174:439–453
7. Ogu EC, Adekunle Y (2013) Basic concepts of expert system shells and an efficient model for knowledge acquisition. Int J Sci Res India Online 2(4)
8. Ahmad A, Paul A, Rathore M, Chang H (2016) An efficient multidimensional big data fusion approach in machine-to-machine communication. ACM Trans Embedded Comput Syst 15(2):1–25
9. Shehata AER, El-Arsh HY (2018) Lightweight joint compression-encryption-authentication-integrity framework based on arithmetic coding. arXiv preprint arXiv:1804.04300
10. Ahmad A, Paul A, Din S, Rathore MM, Choi GS, Jeon G (2018) Multilevel data processing using parallel algorithms for analyzing big data in high-performance computing. Int J Parallel Prog 46(3):508–527
11. Qureshi KN, Bashir F, Abdullah AH (2017) Provision of security in vehicular ad hoc networks through an intelligent secure routing scheme. in 2017 international conference on frontiers of information technology (FIT). IEEE, pp 200–205
12. Iwakoshi T (2017) On problems in security of quantum key distribution raised by Yuen. In Quantum Information Science and Technology III, vol 10442. International Society for Optics and Photonics, p 1044203
13. Khan IA, Qazi R (2019) Data security in cloud computing using elliptic curve cryptography. Int J Comput Commun Netw 1(1):46–52
14. Qayyum S, Naveed A (2019) Cyber physical system based crime resistant model for smart cities. Int J Comput Commun Netw 1(2):19–26
15. Kumar SN (2015) Review on network security and cryptography. Int Trans Electr Comput Eng Syst 3(1):1–11
16. Crandall D, Cosley D, Huttenlocher D, Kleinberg J, Suri S (2008) Feedback effects between similarity and social influence in online communities. In Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining, pp 160–168
17. Russel S, Norvig P (2013) Artificial intelligence: a modern approach. Pearson Education Limited
18. Al Sabbagh B (2019) Cybersecurity incident response: a socio-technical approach. Department of Computer and Systems Sciences, Stockholm University
19. Esser S, Haider H (2017) The emergence of explicit knowledge in a serial reaction time task: The role of experienced fluency and strength of representation. Front Psychol 8:502
20. Young-Eisendrath P (2018) The Buddhist unconscious (Alaya-vijnana) and Jung's collective unconscious: what does it mean to be liberated from the self? In Depth Psychology and Mysticism. Springer, pp 269–282
21. Dennett D (2010) Will AI achieve consciousness? Wrong question. Wired (Feb 9) https://www.wired.com/story/will-ai-achieve-consciousness-wrong-question/. Accessed on 13 June 2019
22. Burr C, Cristianini N, Ladyman J (2018) An analysis of the interaction between intelligent software agents and human users. Mind Mach 28(4):735–774
23. Li D, Gao H (2018) A hardware platform framework for an intelligent vehicle based on a driving brain. Engineering 4(4):464–470
24. Rolls ET (2014) Emotion and decision-making explained: a précis. Cortex 59(185):93
25. Wang P, Liu K, Dougherty Q (2018) Conceptions of artificial intelligence and singularity. Information 9(4):79
26. Fuchs T (2006) Ethical issues in neuroscience. Curr Opin Psychiatry 19(6):600–607
27. Vernon D (2016) Reconciling constitutive and behavioural autonomy. The challenge of modelling development in enactive cognition. Intellectica 65(1):63–79
28. Öğmen H, Herzog MH (2016) A new conceptualization of human visual sensory-memory. Front Psychol 7:830
29. Cooper D (2003) Psychology, risk and safety. Prof Saf 48(11):39–46
30. Banich MT, Mackiewicz KL, Depue BE, Whitmer AJ, Miller GA, Heller W (2009) Cognitive control mechanisms, emotion and memory: a neural perspective with implications for psychopathology. Neurosci Biobehav Rev 33(5):613–630
31. Ramos T, Marques J, Garcia-Marques L (2017) The memory of what we do not recall: dissociations and theoretical debates in the study of implicit memory. Psicológica